FINACAP
CONSULTORIA FINANCEIRA E MERCADO DE CAPITAIS

MANUAL DE CONTROLES INTERNOS

Última revisão: Jan/19
Início de vigência: Jan/15

Diretor de Risco/Compliance

SUMÁRIO

Fazem parte do Manual de Controles Internos:

ASPECTOS GERAIS

1. Introdução

A Finacap tem o compromisso de zelar pela reputação de seus negócios e de sua imagem, assim como preservar os laços de confiança que mantém com seus colaboradores, clientes e prestadores de serviços.

Para mantermos o bom conceito adquirido foi desenvolvido o Código de Conduta e Ética. O intuito do Código é documentar os direitos e deveres das partes relacionadas com a Finacap.

O Código de Conduta e Ética serve como referência para pautar nossas atitudes no dia a dia profissional visando de maneira clara e correta a forma mais adequada de desenvolvermos nossas atividades, com o compromisso de propiciar um ambiente ético, transparente e justo e de adequada gerência de nossos processos e excelência na prestação de serviços em gestão de carteira de terceiros. Além disso, nosso Código de Ética estabelece regras que nos ajudam a atender aos objetivos dos nossos clientes e evitar práticas que possam ferira a nossa relação fiduciária com os mesmos.

O Código fornece as principais diretrizes que devem ser seguidas no que diz respeito a regras internas e externas de conduta por nossos sócios, colaboradores, agentes autônomos de investimento e prestadores de serviços.

A leitura deste manual é obrigatória a todos os prestadores de serviços, agentes autônomos contratados e colaboradores da Finacap.

2. Dúvidas e Procedimentos em Relação ao Código de Conduta e Ética

O Código procura contemplar todas as possíveis questões relacionadas às práticas e procedimentos, mas certamente, existirão certamente casos não previstos. Nestes casos solicitamos que seja procurada orientação adicional com o gestor de sua área.

Em caso de indícios de descumprimento do Código o superior imediato e a Diretoria de Risco e *Compliance* devem ser imediatamente informados.

3. Avaliação da Conduta e Penalidades

Caso sejam reportados indícios de descumprimento do Código o assunto será tratado no ambiente do Comitê de Riscos que irá conduzir as averiguações necessárias para a confirmação da conduta irregular. O Comitê poderá adotar as seguintes medidas: advertência privada; afastamento temporário do cargo; afastamento definitivo do cargo; demissão; rescisão de contrato para agentes autônomos ou prestadores de serviços.

4. Responsabilidade pelo Patrimônio da Empresa

Todo colaborador, agente autônomo ou prestador de serviço ao utilizar os recursos disponibilizados pela Finacap é responsável pela proteção e conservação destes, sejam bens tangíveis ou intangíveis.

5. Conduta em Relação ao Uso de *E-mail*, *Internet*, Sistemas de Informática e Senhas

A Finacap disponibiliza endereço eletrônico a todos os seus colaboradores. A sua utilização deve estar afeita a questões relacionadas às atividades profissionais sendo, no entanto, permitida a utilização pessoal de forma moderada.

Os *e-mails* corporativos enviados ou recebidos, seus respectivos anexos bem como os arquivos constantes nos computadores de propriedade da Finacap poderão ser monitorados.

Os *e-mails* corporativos recebidos, quando abertos, deverão ter sua adequação às regras deste Código imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou o arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

É permitida a utilização de programas de conversas eletrônicas, *chats* externos, gratuitos ou não, para fins comerciais da Finacap. A utilização pessoal, desde que não implique desvio repetido das atividades e responsabilidades, não desrespeite as orientações deste Código e utilizado de forma moderada, é permitida.

A navegação pela rede mundial de computadores, *internet*, deverá ser feita observando as atividades fins da Finacap, sendo permitido o seu uso para fins pessoais de forma moderada. O acesso a *sites* da *internet* inapropriados ou que firam a moral e os bons

costumes serão bloqueados. Toda a navegação na *internet* poderá ser monitorada pela Finacap.

Os colaboradores da Finacap deverão zelar pela conservação do computador utilizado, devendo para tanto realizar periodicamente a verificação da existência de vírus, bem como a manutenção do antivírus atualizado. Sendo constatada a presença de vírus ou qualquer anomalia, deverá comunicar imediatamente o responsável da área e/ou a área de TI.

O recebimento de *e-mails* com arquivos anexados, *links* e principalmente quando não solicitados, devem ser tratados com suspeita e, assim, removidos sem serem abertos, porque é esta a forma mais comum de contágio por vírus.

A Finacap utiliza o *software* Kaspersky Anti Vírus para proteção contra vírus em todos os seus equipamentos. Nos ambientes de rede, a critério da Diretoria responsável, as portas das estações de trabalho poderão ser desabilitadas, visando eliminar a instalação ou geração de cópias piratas e a proliferação de vírus.

As senhas, de caráter sigiloso, pessoal e intransferível serão fornecidas aos colaboradores da Finacap para acesso aos computadores, à rede e ao correio eletrônico corporativos. Em nenhuma hipótese as senhas deverão ser transmitidas a terceiros. Todas as atividades são registradas e associadas à senha do usuário, de modo a responsabilizá-lo no caso de irregularidades.

Caso o colaborador necessite se ausentar do seu local de trabalho, deverá bloquear ou se desconectar do seu computador ou terminal evitando que outras pessoas possam utilizá-lo em seu lugar.

A área de TI será a única autorizada a atribuir senhas de acesso. O *login* à rede deverá identificar claramente seu detentor, na forma como ele é reconhecido na Finacap, através da representação de seu nome. O controle de acesso à rede será atribuído conforme o usuário (níveis de acesso) e monitorado, preferencialmente, via *software*.

6. Uso da Telefonia

É admitida a imprescindibilidade de ligações telefônicas particulares, não significando que a ausência de bom senso em sua utilização por parte dos colaboradores possa ser tolerada. Ligações pessoais interurbanas e para celulares devem durar o tempo estritamente necessário e deverão ser reembolsadas.

As operações cursadas pelas mesas de operações da Finacap são gravadas conforme as exigências das normas vigentes. As atividades ligadas ao sistema de gravação estão descritas no Processo 9. Operações da Mesa de Renda Variável.

É expressamente proibida a utilização de telefone celular no ambiente das mesas de operações.

7. Conduta em Relação às Atividades Desenvolvidas

É vedado aos colaboradores:

1. Utilizar material, marca e logotipo da Finacap e suas empresas afiliadas para assuntos não corporativos ou após o rompimento do vínculo com a empresa;
2. Utilizar quaisquer informações recebidas em função da atividade exercida em benefício próprio ou de pessoas próximas (pais, familiares e amigos);
3. Permitir que clientes ou prestadores de serviço circulem pelas dependências da Finacap desacompanhados de um representante da empresa.

8. Conduta em Relação aos Documentos Produzidos, Correspondências Recebidas e Sigilo de Informações

Todo colaborador é responsável pela exatidão das informações contidas nos relatórios emitidos sob sua responsabilidade.

Todos os papéis e documentação relacionados à empresa e seus clientes deverão ser mantidos em local seguro, de modo a minimizar o risco de que pessoas não autorizadas venham a ter acesso a informações confidenciais. Quando não forem mais necessários devem ser inutilizados (triturados), de modo a impossibilitar a sua reconstituição.

Os colaboradores devem zelar pela confidencialidade de quaisquer informações a que tiverem acesso, que tenham obtido ou tomado conhecimento em função das atividades que desempenham ou desempenharam. Não deve ser transmitida nenhuma informação relativa às operações em andamento ou informações recebidas de pessoas que sejam especialistas em mercado financeiro, cuja publicidade possa influenciar o mercado.

Os colaboradores quando contratados pela Finacap são conscientizados quanto à necessidade de confidencialidade das informações e assinam termo (Termo de Adesão – Código de Conduta e Ética) se comprometendo, na vigência do Contrato de Trabalho e também após a rescisão deste, manter sob sigilosa exclusividade e confidencialidade todas

as informações a que tiver acesso, tais como; dados cadastrais, saldo em custódia, saldos em conta corrente, posição das carteiras de clubes e fundos de investimentos, etc.

Os colaboradores não estão autorizados a discutir informações confidenciais em locais públicos ou através de telefone celular ou viva-voz. De acordo com a legislação brasileira, a divulgação de informações confidenciais ou privilegiadas causando dano a outrem, constitui crime tipificado nos artigos 153 e 154 do Código Penal e artigo 12 da Lei 7.492/86 e na Lei Complementar nº 105.

9. Conduta em Relação às Informações Privilegiadas e Operações no Mercado de Capitais

É vedado aos colaboradores qualquer tipo de operação no mercado financeiro que seja realizada de posse de informação privilegiada. Por informação privilegiada, entende-se qualquer informação que não tenha sido divulgada ao público em geral. Maiores informações sobre operações por sócios, empregados e colaboradores podem ser encontradas na Política de Investimentos Pessoais da Finacap.

10. Conduta em Relação aos Clientes

Os colaboradores devem adotar os seguintes padrões de conduta:

1. Atender os clientes com eficiência, respeito e cortesia, buscando oferecer produtos e serviços adequados às suas necessidades;
2. Prezar pela transparência nas operações realizadas;
3. Fornecer aos clientes informações claras, precisas e adequadas, alertando-os: sobre os riscos inerentes a cada tipo de operação e aplicação em que estejam envolvidos;
4. Manter sigilo sobre quaisquer informações recebidas ou que venham a tomar conhecimento em razão do cargo exercido;
5. Manter contato próximo aos clientes, de forma a conhecer as atividades exercidas pelos mesmos e a origem de seus recursos, para cumprimento da legislação relacionada a crimes de lavagem de dinheiro. É dever dos colaboradores comunicar qualquer suspeita de indício de lavagem de dinheiro a sua gerência;
6. Jamais favorecer um cliente em detrimento de outro.

11. Conduta em Relação aos Prestadores de Serviços

A escolha e a contratação de prestadores de serviços devem ser baseadas em critérios técnicos, imparciais e de acordo com as necessidades da instituição. Deve ser submetida à aprovação da Secretaria a contratação de qualquer empresa na qual um ou mais colaboradores tenham algum tipo de participação ou interesse, direta ou indiretamente.

12. Conduta em Relação aos Órgãos Reguladores e Auditorias Internas e Externas

Todos os colaboradores devem auxiliar e serem diligentes no atendimento de procedimentos decorrentes de exigências de quaisquer órgãos reguladores, auditorias internas ou externas. É vedado aos colaboradores, sem autorização prévia da Diretoria responsável, repassar qualquer tipo de informação aos órgãos reguladores ou auditores.

Caso sejam verificados indícios de violação da legislação que incumbe à CVM fiscalizar, a Finacap informará ao órgão dentro de 10 (dez) dias úteis detalhes da ocorrência ou identificação.

13. Conduta em Relação à Imprensa

É vedado aos colaboradores manifestar-se em nome da Finacap sem autorização prévia da Diretoria de Risco e *Compliance*.

14. Conduta em Relação à Observância da Segregação de Funções - *Chinese Wall*

A denominação *Chinese Wall* é dada ao conjunto de procedimentos e políticas internas de instituição financeira administradora / gestora de fundos e clubes de investimento ou carteiras visando estabelecer uma barreira à comunicação entre diferentes indivíduos ou setores da instituição de modo a assegurar o cumprimento das normas vigentes expedidas pelos reguladores.

As normas exigem a segregação da administração de ativos financeiros de terceiros de forma que os diversos gerenciadores destes recursos não se comuniquem com os gestores dos ativos próprios da instituição. É a separação clara entre a administração dos recursos próprios (tesouraria da instituição financeira) e a administração ou gestão dos recursos de terceiros feitos por veículos de aplicação coletivos.

O objetivo é evitar o conflito de interesse e impedir, por exemplo, que gerenciadores de ativos distintos se misturem e passem a combinar ou simular operações que possam beneficiar a si próprios ou à instituição (tesouraria) ou, ainda, a um ou alguns investidores ou clientes em detrimento de outros.

Assim, a gestão ou administração de carteira, fundos e clubes de investimento está totalmente segregada das áreas/funções da Finacap. A gestão dos recursos das carteiras administradas, clubes e fundos de investimentos são realizados pela Finacap Consultoria Financeira e Mercado de Capitais.

As instalações Finacap Consultoria Financeira e Mercado de Capitais são segregadas fisicamente da área de operação da Finacap. Os sistemas utilizados pela área de gestão são acessados através do uso de senhas e de controle de acesso. Os relatórios e estudos são de uso exclusivo das pessoas envolvidas na área de gestão.

Relatórios envolvendo posição de clientes são confidencias e aqueles que não ficam arquivados são destruídos. Os administradores e funcionários são constantemente alertados quanto à necessidade de sigilo das informações as quais tenham acesso.

A Finacap tem como política relacionada à compra e venda de valores mobiliários por parte dos diretores, gestores e colaboradores (pessoas vinculadas):

1. Dar prioridade na execução das ordens às Carteiras Administradas, Clubes e Fundos de Investimentos;
2. As ordens dos clientes vinculados à Finacap são obrigatoriamente especificadas quando da sua colocação no sistema de negociação;
3. Os clientes vinculados não poderão atuar na contraparte de ordens das carteiras administradas, clubes e fundos de investimentos.

15. Relacionamento Empresa e Colaboradores, Agentes Autônomos e Prestadores de Serviço

O relacionamento entre a Finacap, seus colaboradores, agentes autônomos e prestadores de serviço estão baseados no senso de justiça, respeito mútuo, valorização do ser humano, transparência e compartilhamento de responsabilidades.

Qualquer tipo de discriminação relacionado à origem, raça, religião, classe social, sexo, cor, idade, incapacidade física e quaisquer outras formas de discriminação são considerados atos incoerentes com os valores da empresa e com a cultura de respeito que cada colaborador deve possuir.

As relações no ambiente de trabalho devem pautar-se pela cortesia, pela honestidade, pela integridade e pelo respeito mútuo, independente do cargo ou posição ocupada.

16. Termo de Ciência e Compromisso

Todos os colaboradores, agentes autônomos e prestadores de serviço deverão ler atentamente o Código de Conduta e Ética, preencher e assinar o Termo de Ciência e Compromisso.

1. Política de Segurança de Informação

Este Manual de Segurança da Informação e de Continuidade de Negócios da Finacap contém as Políticas de Segurança de Informação e tem por finalidade garantir de forma geral que as informações geradas e armazenadas no ambiente da instituição estão devidamente protegidas de forma clara e completa, assegurando a continuidade, a confidencialidade, a integridade e a disponibilidade dos seus negócios, atendendo assim, todas as necessidades básicas do mercado e da regulamentação vigente.

O cumprimento desta política é dever de todos os colaboradores e prestadores de serviço da Finacap. A Diretoria Risco e *Compliance* e o *BackOffice*, em conjunto, tem a responsabilidade de estabelecer, definir, implementar e incentivar ações específicas sobre a segurança da informação.

FUNÇÃO	ALOCAÇÃO
DIRETORIA	Diretoria Risco
CONSULTORES	TI / Controladoria
COLABORADORES	Backoffice / Análise

Compete a Diretoria:

- Aprovar Políticas, Normas e Procedimentos relacionados à Segurança da Informação;
- Acompanhar as ações de melhoria contínua nas medidas de proteção visando mitigar os riscos identificados;
- Consistir aspectos de segurança na relação entre estratégias de negócios e evolução tecnológica;
- Aprovar os controles internos e ferramentas utilizadas para garantir a segurança da informação;
- Aplicar penalidades às violações identificadas;
- Incentivar a conscientização sobre Segurança da Informação junto aos colaboradores e prestadores de serviço da Finacap;

- Divulgar aos colaboradores e mantê-los constantemente informados, por meio de correio eletrônico, acerca de fatos que possam comprometer a segurança da informação da Finacap.

O proprietário da informação é o gestor da área de negócio e tem como responsabilidade a manutenção de medidas apropriadas a segurança e a proteção da informação, cabendo a este delegar aos usuários autorização para acessar as informações, sem, contudo, deixar de responder pela responsabilidade final de proteção da informação.

Cabe a ele autorizar o responsável pela área de TI a liberar o acesso às informações solicitadas pelos usuários / colaboradores da Finacap. As solicitações e autorizações deverão ser realizadas por meio de correio eletrônico para que fiquem documentadas.

Compete ao Colaborador:

- Salvaguardar toda informação da Finacap criada ou utilizada na execução de suas atividades, incluindo revelação não autorizada, modificação ou destruição;
- Conhecer as leis e regulamentos aplicáveis ou relacionados à segurança da informação, às informações criadas, usadas ou adquiridas como: direito de propriedade e licença de *software*;
- Não utilizar os recursos de tecnologia da Finacap de forma ilegal, antiética ou não autorizada como: arquivos pornográficos, correntes, jogos, *softwares* não autorizados, etc.

São consideradas violações à Política de Segurança da Informação as seguintes situações, não se limitando às mesmas:

- Quaisquer ações ou situações que possam expor a Finacap, direta ou indiretamente, à perda financeira ou de imagem;
- Uso indevido de dados corporativos, equipamentos, *software*, divulgação não autorizada de informações, sem a permissão expressa do proprietário da informação / gestor da área de negócios;
- A não comunicação imediata à diretoria responsável de quaisquer violações ou atitudes anormais que porventura venha a tomar conhecimento ou chegue a presenciar.

A não aderência a Política de Segurança da Informação e suas definições são consideradas faltas graves podendo inclusive ser passível de:

- Aplicação de sanções trabalhistas previstas em legislação vigente, incluindo dispensa por justa causa ou afastamento;
- Término ou cessão do contrato de prestação de serviços ou relação comercial;
- Ressarcimento dos prejuízos causados à Finacap conforme previsto em contrato com empresas de prestação de serviços ou aplicação de outras ações disciplinares constantes na legislação vigente.

2. Sistemas de Informação

São considerados como parte do Sistema de Informação da Finacap todos os programas de informática, incluindo, os *e-mails*, os sistemas instalados nos computadores de propriedade da Finacap, bem como os bancos de dados que a Finacap utiliza para o armazenamento de suas informações e de seus clientes e os sistemas que venham a ser desenvolvidos, direta ou indiretamente, pela equipe de membros da Finacap ou de instituições afiliadas.

Os sistemas desenvolvidos, em desenvolvimento ou que venham a ser elaborados pelos colaboradores constituem propriedade exclusiva da Finacap, cabendo à mesma as decisões acerca de sua comercialização, reprodução e utilização.

Os equipamentos e os computadores de propriedade da Finacap, bem como os bancos de dados utilizados que forem disponibilizados aos colaboradores deverão ser utilizados de forma a atender exclusivamente às finalidades da Finacap. A obtenção de cópias de arquivos de qualquer extensão, de forma gratuita ou remunerada, em computadores da Finacap, originados em máquina remota, *download,* depende de autorização expressa e prévia da área responsável e deverá observar os direitos de propriedade intelectual pertinentes, tais como: *copyright*, licenças e patentes.

Em hipótese alguma será permitida a cópia de *softwares* piratas ou que não respeitem direitos de propriedade intelectual.

3. Segurança da informação

A informação é um dos principais patrimônios do mundo dos negócios. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento. Mas esse

poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos a FINACAP e prejudicar nosso crescimento e vantagem competitiva. Atentos a isso, publicamos a Política de Segurança da Informação, o alicerce dos esforços de proteção à informação da FINACAP.

Segurança da Informação são esforços contínuos para a proteção dos ativos de informação, auxiliando o FINACAP a cumprir sua missão. Para tanto, visa atingir os seguintes objetivos:

- **Confidencialidade**: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

- **Integridade**: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

- **Disponibilidade**: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

4. Proteção da Informação

A informação é um importante ativo para a operação das atividades comerciais e para manter a vantagem competitiva no mercado. Tal como os ativos da FINACAP, a informação deve ser adequadamente manuseada e protegida.

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Toda informação relacionada às operações da FINACAP, gerada ou desenvolvida nas dependências da FINACAP, durante a execução das atividades, constitui ativo desta instituição financeira, essencial à condução de negócios, e em última análise, à sua existência.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

A modificação, divulgação e destruição não autorizadas e oriundas de erros, fraudes, vandalismo, espionagem ou sabotagem causam danos aos negócios da FINACAP.

É diretriz que toda informação de propriedade da FINACAP e seus clientes sejam protegidas de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

4.1 Responsabilidades

É missão e responsabilidade de cada um, seja por meio de seu funcionário, estagiário, prestador de serviços, parceiro ou visitante, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação. É imprescindível que cada colaborador compreenda o papel da segurança da informação em suas atividades diárias.

Todas as atividades executadas pela FINACAP, por meio de seus funcionários, estagiários e demais colaboradores, devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras, com relação à segurança da informação.

Para auxiliar a todos os colaboradores nessa missão, a FINACAP criou a **Diretoria Risco e *Compliance* e o *BackOffice***, que administra as disciplinas de conhecimento que dão suporte a essa ciência. Essa Comissão é responsável por editar as políticas e padrões que apoiam a todos na proteção dos ativos de informação, e está preparada para auxiliar na resolução de problemas relacionados ao tema.

Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações das partes consideradas não disponível ao público ou reservadas, dados, contratos, dados dos clientes, manuais, esboços, modelos, amostras, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela FINACAP em decorrência da execução do contrato de prestação de serviços.

São responsáveis pela observância desta Política os diretores, empregados, agentes e consultores (incluindo advogados, auditores e consultores financeiros).

O Colaborador que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento por escrito da FINACAP. Qualquer revelação das informações confidenciais deverá estar de

acordo com os termos e condições estabelecidos pela FINACAP. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades.

O Colaborador deverá resguardar as informações confidenciais de forma estrita, e jamais poderá revelá-las a não ser para os seus representantes legais. A parte que receber as informações será responsável por qualquer não cumprimento desta Política porventura cometido pelos seus representantes legais.

O Colaborador deverá informar prontamente a FINACAP sobre qualquer uso ou revelação indevida da informação ou qualquer outra forma que caracterize o descumprimento desta Política.

Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política:

(i) O atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunal arbitrais e de órgãos públicos administrativos;

(ii) A divulgação das informações confidenciais aos agentes, representantes (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e empregados das partes; e,

(iii) As informações confidenciais que forem divulgadas somente após o consentimento, por escrito, do FINACAP.

Se a qualquer uma das partes ou seus representantes legais, que detém as informações confidenciais, for solicitado ou requerido, oralmente ou por escrito, solicitações de informações de documentos, mandados de investigações civis ou qualquer outro pedido similar, para revelar tais informações confidenciais, deverá notificar prontamente a outra parte para que esta tenha tempo hábil para verificação, inclusive, se for o caso, aplicar as ressalvas contidas nos termos desta Política.

As cláusulas de ciência, responsabilidade e confidencialidade quanto à política e diretrizes de segurança da informação visam alertar e responsabilizar o Colaborador de que o acesso e o manuseio de informação devem se restringir ao exercício da função ou processo que requer essa informação, sendo proibido o uso para qualquer outro propósito distinto do designado.

4.2 Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de Segurança da Informação, por qualquer meio. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar sanções:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas;

Os princípios de segurança estabelecidos na presente política possuem total aderência da administração da FINACAP e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta política e a violação de normas derivadas da mesma sujeita os Colaboradores às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos.

Em caso de dúvidas quantos aos princípios e responsabilidades descritas nesta norma, o Colaborador deve entrar em contato com a Comissão.

5. Classificação da Informação

As informações e os sistemas de informação, diretórios de rede e bancos de dados são classificados como estritamente confidenciais.

As informações, seja no período de geração, guarda, uso, transferência e destruição devem ser tratadas em conformidade com cada etapa do ciclo.

As informações confidenciais necessitam de sigilo absoluto e devem ser protegidas pelo colaborador de alterações não autorizadas e estarem disponíveis apenas às pessoas pertinentes e autorizadas a trabalhá-las, sempre que necessário. Cabem ao colaborador todos os esforços necessários de segurança para protegê-las.

Falhas no sigilo da informação, integridade ou disponibilidade deste tipo de informação trazem grandes prejuízos à Organização, expressos em perdas financeiras diretas, perdas de competitividade e produtividade ou imagem da FINACAP, podendo levar à extinção das operações ou prejuízos graves ao crescimento.

São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.), situação financeira e movimentação bancária;

- Informações sobre produtos e serviços que revelem vantagens competitivas do FINACAP frente ao mercado;

- Todo o material estratégico da FINACAP (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);

- Quaisquer informações da FINACAP, que não devem ser divulgadas ao meio externo antes da publicação pelas áreas competentes;

- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

Classificação	Transporte	Armazenamento	Transmissão	Destruição	Rastreamento
Confidencial	Envelopes lacrados e assinado em suas abas evitando violações	Criptografado no servidor de arquivos com acesso restrito a Diretoria e Pessoas autorizadas por eles.	Sempre de forma segura através de VPN ou E-mail.	Picotadeira acompanhada por pessoa da diretoria	Protocolo com número único e código de rastreamento.
Restrito	Envelopes lacrados e assinado em suas abas evitando violações	Criptografado no servidor de arquivos com acesso restrito a Diretoria e Pessoas autorizadas por eles.	Através de e-mail seguro	Picotadeira acompanhada por pessoa da diretoria	Protocolo com número único e código de rastreamento.
Publico	Envelope lacrado	No servidor de arquivo	Por e-mail	Picotadeira	Protocolado.

A criptografia é feita com o software AxCrypt usando algoritmo AES de 128 bits para criptografas os arquivos.

6. Acesso a Sistemas e Recursos de Rede

O colaborador é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização destes poderes.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.

6.1 Direito de Acesso (Autorização)

O Colaborador é o responsável pela utilização e eventuais usos inadequados dos direitos de acesso que são atribuídos.

A solicitação de acesso à informação assim como suas modificações deve decorrer da necessidade funcional do Colaborador e deverá ser autorizada e controlada pelo seu superior imediato, registrado sempre por meio eletrônico.

Todo colaborador deverá ser registrado no domínio com identificador único e senha intrasferível.

A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função. Periodicamente, os acessos concedidos devem ser revistos pelos Gestores.

Em caso de demissão, o acesso deverá ser retirado ao mesmo tempo do aviso de desligamento do colaborador.

Todas as atividades são registradas e associadas à senha do usuário, de modo a responsabilizá-lo no caso de irregularidades. Caso o colaborador necessite se ausentar do seu local de trabalho, deverá bloquear ou se desconectar do seu computador ou terminal evitando que outras pessoas possam utilizá-lo em seu lugar.

A área de TI será a única autorizada a atribuir senhas de acesso. O “Login” à rede deverá identificar claramente seu detentor, na forma como ele é reconhecido na Finacap, através da representação de seu nome. O controle de acesso à rede será atribuído conforme o usuário (níveis de acesso) e monitorado, preferencialmente, via software.

Os acessos estão implementados da conforme abaixo:

- Tentativas de acesso antes do bloqueio → 5 vezes;

- O sistema se alto bloqueia em 30 min;
- A senha expira com 90 dias solicitando nova senha;
- O PFSENSE, está implementado para registrar todos os logs de acesso à rede.

6.2 Utilização dos Recursos de Informação

Apenas os equipamentos e software disponibilizados e/ou homologados pela FINACAP podem ser instalados e conectados à rede da FINACAP. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

Autenticação e Senha:

O colaborador é responsável por todos os atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Os colaboradores devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum. Ou seja, não contá-la a ninguém e não anotá-la em papel;

- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;

- Selecionar senhas de qualidade, que sejam de difícil adivinhação combine maiúsculas, minúsculas, números e caracteres não alfanuméricos com 8 caracteres;

- Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;

- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

7. Direitos de Propriedade

Todo produto resultante do trabalho dos Colaboradores (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da FINACAP. Em caso de extinção ou rescisão do contrato de prestação de serviços de Colaborador, por qualquer motivo, deverá o Colaborador devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços ao FINACAP, ou emitir declaração de que as destruiu.

Para evitar que o Colaborador guarde em seu poder quaisquer arquivos, todos os documentos e suas versões devem ser guardadas nos servidores de arquivo da FINACAP em pastas protegidas e com acesso restrito.

8. Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Organização.

9. Mesa Limpa

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

10. Conversas em Locais Públicos e registro de informações

Não discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de texto, exceto quando encaminhadas a FINACAP.

11. Leis e Regulamentos

É de responsabilidade do Colaborador conhecer a legislação e cumprir os requisitos legais, normas e padrões locais vigentes.

12. Endereço Eletrônico, Acesso à *Internet*, Política Antivírus

A Finacap disponibiliza endereço eletrônico a todos os seus colaboradores, sendo tal endereço eletrônico destinado para fins exclusivamente corporativos. A utilização do endereço eletrônico deverá ser feita para questões relacionadas às atividades profissionais sendo, no entanto, permitida a utilização pessoal de forma moderada. Os e-mails corporativos enviados ou recebidos, bem como seus respectivos anexos e os arquivos constantes nos computadores de propriedade da Finacap poderão ser monitorados pela Finacap.

Os e-mails corporativos recebidos, quando abertos, deverão ter sua adequação às regras desta Política imediatamente verificada. Não será admitida, sob qualquer hipótese, a manutenção ou o arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

A navegação pela rede mundial de computadores, internet, deverá ser feita observando as atividades fins da Finacap, sendo permitido o seu uso para fins pessoais de forma moderada. O acesso a sites da internet inapropriados ou que firam a moral e os bons costumes serão bloqueados. Toda a navegação na internet poderá ser monitorada pela Finacap.

Os colaboradores da Finacap deverão zelar pela conservação do computador utilizado, devendo para tanto realizar periodicamente a verificação da existência de vírus, assim como a manutenção do antivírus atualizada. Sendo constatada a presença de vírus ou qualquer anomalia, deverá comunicar imediatamente o responsável pela área.

O recebimento de e-mails com arquivos anexados, links e principalmente quando não solicitados, devem ser tratados com suspeita e, assim, removidos sem serem abertos, porque é esta a forma mais comum de contágio por vírus.

A Finacap utiliza o software Kaspersky Anti Vírus para proteção contra vírus em todos os seus equipamentos. Nos ambientes de rede, a critério da Diretoria responsável, as portas das estações de trabalho poderão ser desabilitadas, visando eliminar a instalação ou geração de cópias piratas e a proliferação de vírus.

13. Telefonia e Manutenção de Sistema de Gravação

As operações cursadas pelas mesas de operações da Finacap são gravadas conforme as exigências das normas vigentes.

É expressamente proibida a utilização de telefone celular no ambiente das mesas de operações.

É admitida a imprescindibilidade de ligações telefônicas particulares, não significando que a ausência de bom senso em sua utilização por parte dos colaboradores possa ser tolerada. Ligações pessoais interurbanas e para celulares devem durar o tempo estritamente necessário e deverão ser reembolsadas.

14. Avaliação e Compra de *Hardware* e *Software*

Nenhum *hardware* ou *software* poderá ser adquirido e/ou instalado na Finacap sem autorização da Diretoria de Risco e *Compliance*. Antes de ser comprado, todo *hardware* e *software* será avaliado diretamente pela área de TI, quanto a:

- Viabilidade técnica e aderência à plataforma tecnológica;
- Facilidade de manutenção;
- Documentação;
- Atendimento às necessidades da Finacap.

Complementará essa avaliação, a verificação da procedência do *hardware* ou do *software* e, tratando-se de *software*, a existência de Licença de Uso.

O gestor da área de TI deverá avaliar a necessidade de confecção de uma SLA com o fornecedor do *hardware* ou *software*, conforme estabelecido no Código de Conduta e Ética.

15. Impressão de Documentos

Qualquer relatório que contiver informações confidenciais da Finacap ou de seus clientes são mantidos arquivados adequadamente e, os que porventura se destinarem ao lixo, serão obrigatoriamente destruídos com antecedência. Documentos impressos e não utilizados são todos destruídos antes de serem depositados no lixo.

16. *Backup* e Segurança dos Arquivos

Os backups de arquivos/dados referentes às carteiras administradas são gravados diariamente.

O descarte dos meios magnéticos substituídos utilizados para gravação de arquivos (de backup ou não) será efetuado somente pelos colaboradores autorizados, através de fragmentação ou desgravação de seu conteúdo.

17. Segurança do *Hardware*

Os nobreaks são devidamente dimensionados, para garantir:

- A uniformidade da tensão da rede, em casos de picos de energia;
- No mínimo, o salvamento dos dados e o desligamento apropriado dos equipamentos, nas faltas de energia elétrica.

18. Plano de Contingência

Os arquivos de backup são armazenados em local diferente ao do escritório, em local seguro e de acesso somente aos colaboradores autorizados.

Em caso de sinistro nas instalações, a Finacap utilizará notebooks com acesso à internet e aos programas ou softwares utilizados por suas áreas de negócio e telefones celulares para dar andamento as suas atividades ou operações diárias.

Esse plano deverá ser revisado todas as vezes que tivermos lições aprendidas e ou quando houver a necessidade de atualizações.

O tempo máximo de interrupção deverá ser de 1h, neste período o setor de TI deverá analisar as causas de interrupção, verificar as possibilidades, comunicar a Comissão e a Diretoria tomando assim em conjunto as ações necessárias para sanar essa interrupção de forma definitiva.

18.1 Backup

Os arquivos de backup são armazenados em locais diferentes ao do escritório, em local seguro e de acesso somente aos colaboradores autorizados.

Semanalmente os backups serão testados para garantir sua integridade, a gravação e feita de forma automática nos servidores de arquivos, que contem disco em RAID, espelhados na nuvem.

18.2 Rede

Manutenções ou revisões periódicas minimizam a inoperabilidade da rede interna, no entanto, na eventual pane de rede, o processamento poderá ser efetuado no local (no disco rígido, Hard Disk, da própria estação de trabalho) até o retorno da normalidade da situação.

18.3 Hardware

Na impossibilidade de qualquer equipamento que componha a estação de trabalho funcionar, é efetuada a sua retirada e colocado outro em seu lugar, quando disponível, imediatamente. Então se levanta a possibilidade de conserto por pessoal próprio ou encaminha-se a empresas especializadas para o devido conserto, preferencialmente àquelas que possuem firmadas SLAs, firmadas e assinadas o termo de compromisso de não divulgação dos conteúdos restritos a FINACAP sob pena da LEI.

18.4 Software

Caso não seja possível por qualquer motivo o acesso a software ou programa proprietário, a área de TI procurará corrigir o problema ou proceder a sua reinstalação completa evitando a perda de informação eventualmente já gravada ou arquivada pelo usuário.

18.5 Uso de outros programas e dos computadores

É expressamente proibido a instalação programas não autorizados nas estações de trabalho, entenda-se por programa não autorizado qualquer software que não tenha sido previamente analisado e aprovado pela gestão de TI e disponibilizado no servidor de arquivos local.

19. Proteção de Computadores e Redes

Todo equipamento antes de serem disponibilizado para uso, deverá ter sido alterada a BIOs para não dar boot por qualquer dispositivo móvel assim como inserção de senha para acesso a BIOs.

O próximo passo é o “hardening” da rede. Neste processo foi removido todos os acessos desnecessários no firewall, tanto no sentido “outbound” (de dentro para fora), como no sentido “inbound” (de fora para dentro), de forma a diminuir as possibilidades que um usuário mal-intencionado teria para fazer um ataque.

Além do bloqueio dos acessos desnecessários, os colaboradores devem-se atentar também para a circulação de senhas no modo “texto”, ou seja, de um modo que facilite a captura das mesmas. O SSL que deve ser utilizada sempre que possível.

Para o acesso “inbound”, a área de TI e os colaboradores deveram seguir as seguintes regras:

- Nunca disponibilize um serviço que use autenticação sem que este seja criptografado: SMTP, POP, IMAP devem ser disponibilizados apenas por SSL. O HTTP, dos websites deve ser SSL sempre que houver alguma autenticação envolvida;
- Nunca deixar portas abertas do que o necessário para a sua operação. Se os seus funcionários não podem acessar o e-mail de casa, não deixe a conexão para os serviços POP, SMTP e IMAP abertos;
- Restrinja, sempre que possível, a origem dos acessos a um determinado serviço. Supondo que haja apenas um parceiro de negócios que precise acessar o seu servidor web, então tente fechar o acesso para este parceiro. Se este tiver um IP fixo, configure o acesso por IP. Caso contrário, configure outro tipo de autenticação;
- Sempre as portas-padrão dos serviços;
- Mesmo quando configurado em uma porta diferente, é necessário o mesmo cuidado para bloquear os acessos indevidos.
- Utilize conexões VPN se for necessário dar um acesso mais geral à sua rede, como servidores de disco e impressoras.
- Evitar criar muitos acessos de entrada no seu firewall.

Para proteger o acesso “outbound”, a área de TI e os colaboradores deveram seguir as seguintes regras:

- A regra mais importante é: tudo que não precisa ser permitido deve ser bloqueado. Melhor ainda: comece bloqueando tudo e vá liberando especificamente o que é necessário;
- Usuários internos também podem atacar a sua rede. Embora menos importante, procure utilizar criptografia nos protocolos que exigem autenticação. Para não ter que pagar um certificado SSL para isso, utilize certificados gerados pelo próprio servidor da empresa (Self-signed certificates);
- Preste particular atenção nas conexões HTTPS saindo.
- Quanto ao acesso à navegação, escolha a forma de controle de acordo com o perfil dos profissionais e o tipo de trabalho feito na empresa, sempre bloquear sites suspeitos e sempre está atualizando as black list;
- Quando for necessário utilizar programas que não tem portas e endereços IP de acesso fixos, opte por fazer o controle baseado no nome do programa.

As regras acimas deveram alinhada com as novas tecnologias e com o negócio da FINACAP.

Não é permitido a instalação de softwares piratas nas redes da FINACAP;

O firewall deverá conter todas as regras de bloqueio de sites, e-mail, aplicativos que não sejam homologados pela FINACAP;

O setor de TI deverá sempre manter as atualizações de segurança atualizadas.

As redes wifi da FINACAP escritório deverá ser utilizada apenas pelos funcionários efetivos da empresa, todo e qualquer outro deverá utilizar a rede visitante, as regras de segurança mínimas são:

- Rede Escritório:
  - A segurança deverá está em WPA 2 com AES;
  - Deverá fazer o cadastro dos MAC que utilizam a rede sem fio;
  - Se possível vincular o acesso ao Domínio da Rede.
- Rede Visitante:
  - Utilizar uma página de HotSpot para autenticação dos visitantes;
  - Os visitantes deveram solicitar o voucher e fazer um cadastro na recepção antes de recebe-lo.

Os visitantes que portarem equipamentos moveis dentro do escritório deveram fazer um cadastro na recepção da empresa, e só deveram acessar a rede visitante.

Regras definidas no software antivírus Kapersky:

- Nível de Segurança: Classificar como “Recomendado”;
- Ação ao Detectar Ameaças (Arquivos e E-mails): Classificar como “Automatico”;
- Relatórios: Armazenar por 1 mês com tamanho máximo de 1024 MB;
- Quarentena: Armazenar por no máximo 1 mês;
- Verificação Dispositivos: Completa com volume inferior à 64 GB;
- Agendamento de Verificação: Semanal.

20. Gerenciamento de Mudanças

Após receber o pedido do solicitador da mudança, a Diretoria Risco e *Compliance* e o *BackOffice* ou pessoa por eles designado deve aferir a prioridade da mudança. Em seguida, notificará o Diretoria e conduzirá reuniões com eles regularmente para se garantir que todas as mudanças sejam devidamente tratadas.

Depois de aprovadas as mudanças, a Diretoria Risco e *Compliance* e o *BackOffice* notifica ao gesto da área afetada para providenciar as mudanças e enviá-las para teste.

Após os testes, a Diretoria autoriza sua implantação e informa a todos os que serão afetados por ela, direta e indiretamente.

21. Gerenciamento de Riscos de Fornecedores

A capacidade de um fornecedor atender a demanda com qualidade, bom preço e eficiência de entrega e tempo de resposta para possíveis problemas de logística pode fazer toda a diferença na hora de contar com a matéria-prima ou componentes de determinado produto.

A Finacap deverá responder as perguntas abaixo antes de contratar qualquer fornecedor:

- As empresas que fazem parte da carteira de fornecedores da minha empresa têm uma história sólida no mercado?
- Elas têm capacidade de assumir os compromissos acordados?
- Qual seu grau de endividamento?
- Sua governança combina com os valores da minha empresa?
- Como está a imagem delas e qual seu grau de envolvimento com sustentabilidade e responsabilidade social?

Além disso, a área de compras da FINACAP deverá verificar os antecedentes de todos os fornecedores e isso não isentará o fornecedor de ter conhecimento das regras de proteção a informação da empresa e assinar termo de responsabilidade e conhecimento das regras.

Deve-se alimentar uma planilha com pontuações para os fornecedores fazendo assim um ranking com todos separando por área de aquisição e serviços.

22. Reposte de Incidentes

22.1 Objetivos do Processo

Incidente → Define: " qualquer evento adverso, confirmado ou sob suspeita."

São objetivos da gestão de incidentes:

- Garantir a detecção de eventos e tratamento adequado, sobretudo na categorização destes como incidentes de segurança da informação ou não.
- Garantir que incidentes de segurança da informação são identificados, avaliados e respondidos de maneira mais adequada possível.
- Minimizar os efeitos adversos de incidentes de segurança da informação (tratando-os o mais brevemente possível).
- Reportar as vulnerabilidades de segurança da informação, além de tratá-las adequadamente.
- Ajudar a prevenir futuras ocorrências, através da manutenção de uma base de lições aprendidas (algo parecido com a base dados de erros conhecidos).

22.2 Avaliação e decisão

O principal objetivo aqui é avaliar os eventos de segurança da informação e decisão sobre se é incidente de segurança da informação.

É preciso realizar uma avaliação das informações relevantes associadas com a ocorrência de eventos de segurança da informação e classificar o evento como um incidente ou não.

Subatividades:

- Decidir sobre a classificação (como evento ou incidente);
- Utilizar bases de dados e procedimentos para investigação, assim como manter estas bases e procedimentos atualizados;
- Avaliar a situação com base nas classificações de eventos / incidentes de segurança;
- Identificação de serviços afetados;
- Mensuração dos impactos nos ativos da informação considerando os critérios da informação: confidencialidade, integridade e disponibilidade;
- Classificar e priorizar o incidente / evento;
- Realizar o escalonamento adequado;
- Reportar o evento / incidente a partes interessadas;
- Atribuir as responsabilidades adequadas para o tratamento do incidente / evento;
- Fornecer os procedimentos adequados a cada responsável;
- Outras atividades mais específicas podem ser necessárias para armazenar de forma adequada evidências / provas sobre a causa do incidente (sobretudo em caso de ataques).

22.3 Responder ao incidente de segurança

A partir deste ponto, as atividades descritas já partem do pressuposto de que a ocorrência foi classificada como incidente de segurança e, portanto, este deve ser tratado no contexto do processo.

Subatividades:

- Conduzir ações conforme acordado na atividade de avaliação e decisão (atividade anterior);
- Respostas a incidentes de segurança da informação, incluindo a análise forense;
- Instigar a resposta requerida, independe do responsável por tratá-la;
- Escalonamento para responsáveis por gestão da continuidade, quando o impacto da situação for percebido como desastroso;
- Pode envolver posterior análise forense, se necessário;
- Atualizar todos as partes envolvidas sobre o andamento do tratamento do incidente;
- Dar continuidade a subatividade - citada no item anterior - de recolhimento de provas eletrônicas e armazenada seguro destas, caso seja necessário para a perseguição legal ou disciplinar do autor;
- Resposta para conter e eliminar o incidente de segurança da informação;
- Recuperar serviços impactados.

Toda suspeita de incidente deverá ser reportada ao imediato hierárquico, que deverá reportar e deixar a diretoria informada das suspeitas após um levantamento prévio.

23. Revisão

A presente política deverá ser revisada anualmente.

MANUAL DE NEGOCIAÇÃO DE ATIVOS

1. Introdução

Este manual tem como objetivo reunir as regras e diretrizes que devem ser seguidas em relação à:

I. Gestão de recursos de terceiros na Finacap;

II. Investimentos pessoais por parte de colaboradores da Finacap;

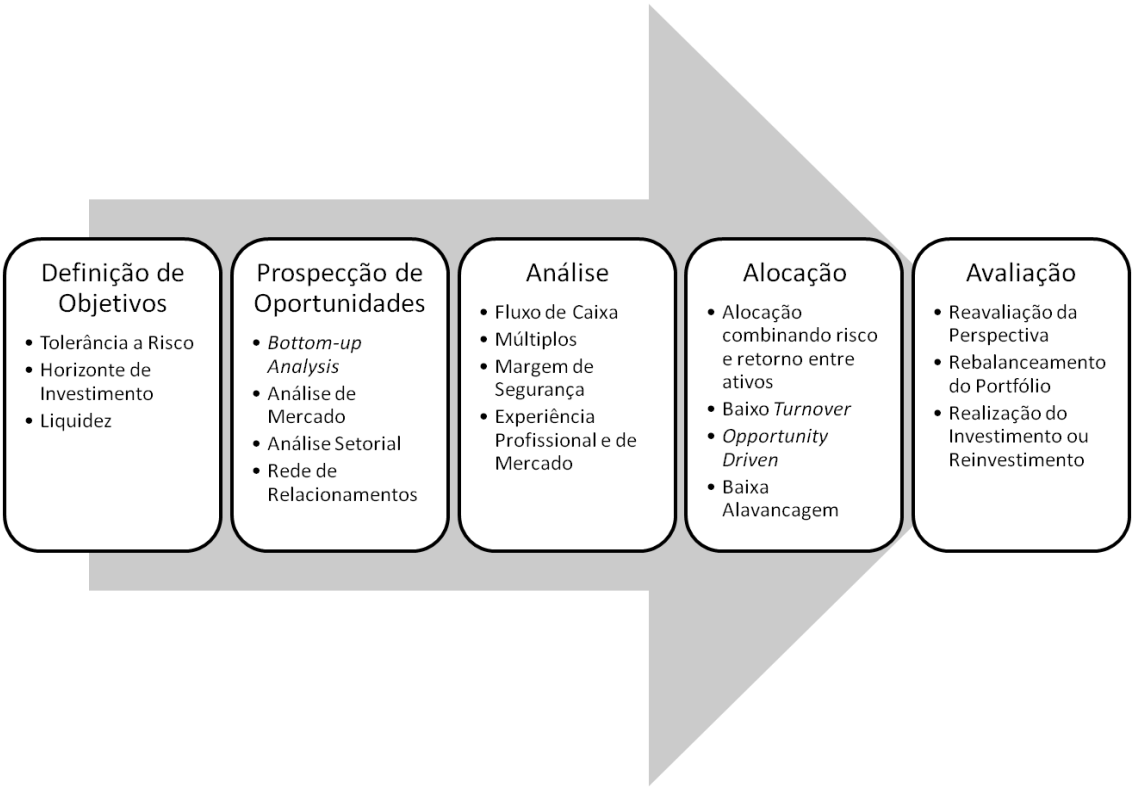
O manual descreve a Filosofia de Investimento, os Princípios e Regras Básicas, procedimentos operacionais e informações necessárias para a execução das ordens de compra e venda de ativos, sejam eles de Renda Variável ou Renda Fixa (Público ou Privado). Além disso, o manual cobre assuntos relacionados aos investimentos pessoais de sócios e colaboradores da Finacap.

2. Propostas e Filosofia de Investimento da Finacap

A proposta da Finacap é implementar e conduzir estratégias de gestão ativas que proporcionem retornos acima da média dos *benchmarks* específicos de cada fundo ou carteira sob gestão. Os *benchmarks* mais comumente utilizados para efeitos de comparação são o Ibovespa, para fundos de Renda Variável, e o CDI, IPCA e a SELIC para fundos de Renda Fixa.

A Finacap adota como filosofia de investimento, a abordagem conhecida como *Value Investing:* Uma estratégia de longo prazo que se propõe a selecionar ativos que apresentem um preço de mercado inferior ao preço justo (valor intrínseco) e a manutenção destes ativos até o momento que eles atinjam ou ultrapassem a barreira do preço justo. Esta filosofia de investimento requer especialmente paciência e disciplina para que os ativos se ajustem aos valores justos, principalmente durante períodos conturbados da economia e do mercado de capitais.

Processo Decisório:



3. Princípios Básicos

I. Não agir, ou provocar terceiros a agir, com base em informação relevante não pública, que possa afetar o valor de um investimento negociado publicamente.

II. Dar prioridade aos investimentos realizados em nome do cliente em relação aos que beneficiam o interesse próprio do gestor.

III. Usar comissões geradas a partir de negócios do cliente para pagar apenas serviços ou produtos que diretamente auxiliam o gestor na sua tomada de decisão de investimento, e não para a administração geral da empresa.

IV. Maximizar o valor da carteira dos clientes, buscando a melhor execução para todas as transações dos clientes.

V. Estabelecer políticas para assegurar a alocação justa e equitativa entre contas de clientes.

4. Regras para Negociação de Ativos

I. O cliente deve estar devidamente cadastrado na corretora que for realizada a negociação.

II. O gestor deverá comunicar a Diretoria de Risco e *Compliance* toda operação em que há dúvida se ela se baseia em informação relevante não pública que possa vir a afetar o valor de um investimento negociado publicamente.

III. Todo material de pesquisa que fundamente as operações executadas para os fundos de investimentos ou carteira de clientes deve ser armazenada e catalogada por um período de pelo menos 2 anos.

IV. Todos os colaboradores devem atestar conhecimento da Política de Investimentos Pessoais.

V. Sempre que houver execução de operação de compra e venda de ativos entre carteiras de clientes e destes com a gestora, o gestor deve comunicar ao *Compliance Officer* as justificativas para a operação.

VI. O gestor deve assegurar que todas as ordens de compra e venda de ativos sejam confirmadas com notas de negociação. Estas devem ser armazenadas e catalogadas nas suas respectivas contas por pelo menos 2 anos.

VII. Apenas as pessoas formalmente autorizadas podem executar ordens em nome dos clientes da gestora. Estas ordens devem ser registradas por meio de gravação eletrônica, quando verbais, ou por protocolo de registro de sistemas de comunicação *on-line*.

VIII. Na seleção das corretoras utilizadas para execução de operações, deverão ser observados diversos aspectos, como: infraestrutura tecnológica, qualidade da equipe de *research*, custo das operações, atendimento especializado, entre outros.

IX. Toda e qualquer vantagem que obtiver junto às corretoras ativas são repassados diretamente para os clientes

X. Anualmente, o gestor deve proceder a reavaliação das condições comerciais e operacionais das corretoras ativas e emitir relatório de situação para o *Compliance Officer*. Este relatório deve especificar um plano de distribuição das ordens entre as corretoras ativas e a justificativa para a seleção das corretoras ativas.

XI. Quando for o caso, o gestor deve usar *block trades* e repartir as cotas de forma pro-rata para garantir que todos os clientes, para os quais o ativo é apropriado, tenham a oportunidade de participar de forma justa e igualitária.

XII. Quando o gestor não receber uma alocação grande o suficiente para permitir que todos os clientes elegíveis participem plenamente em uma oferta particular, ele deve assegurar que certos clientes não recebam tratamento preferencial e deve estabelecer um sistema para garantir que as cotas serão alocadas de forma justa.

XIII. O rateio da quantidade de títulos e valores mobiliários negociados é feito de acordo com os critérios: valor do patrimônio, valor do patrimônio em relação ao perfil de riscos, quantidade total do ativo já presente na carteira de cada cliente, exigências legais da política de investimentos. Caso haja diferenciação de preço, deverá ser usado o preço médio das operações por cada ativo. Esse procedimento deverá ser adotado tanto para fundos de investimento quanto para pessoas físicas ou jurídicas.

XIV. Os percentuais de rateio são calculados de forma manual levando em conta os parâmetros do item acima, e são devidamente informados para área de Risco e Compliance.

5. Regras para Negociação de Títulos de Crédito Privado

Diferentemente dos ativos de Renda Variável e dos Títulos Públicos, os Títulos de Crédito Privado, que emitidos passam a ser negociados no mercado secundário (balcão), frequentemente não tem seus preços definidos por sucessivas negociações de mercado e em tempo real. Dessa forma, Títulos de Crédito Privado apresentam fatores de risco diferenciados quando comparados a outros ativos tradicionais. Isso requer que sejam respeitadas pelos gestores da Finacap, os seguintes procedimentos:

I. Apresentar ao Comitê de Investimento & Riscos os riscos inerentes e as estratégias de controle de risco das operações de Títulos Privados a serem realizadas para prévia ciência e autorização;

II. Dispor do Prospecto da emissão;

III. Dispor do relatório de *rating* e a respectiva súmula do ativo ou do emissor, fornecido por agência classificadora de risco de crédito e dos demais riscos inerentes a emissão do título;

IV. Ter acesso aos documentos integrantes da operação, incluindo informações sobre garantias reais ou fidejussórias e demonstrações financeiras do emissor auditas por auditor independente;

V. Ter acesso às demais informações que o gestor julgar necessárias a devida analise de credito para compra e acompanhamento do ativo;

VI. Submeter a diretoria de Compliance e Risco toda a documentação e o relatório de Análise do Investimento sempre que houver inclusão de novo ativo ou aumento do nível de exposição aprovado por emissor

VII. Monitorar o risco de crédito envolvido na operação, bem como a qualidade e capacidade de execução das garantias, enquanto o ativo permanecer nas carteiras ou fundos geridos;

VIII. Renovar periodicamente, enquanto o ativo permanecer na carteira do fundo, as avaliações do risco de crédito envolvido na operação, bem como da qualidade e capacidade de execução das garantias;

IX. Declarar com devida assinatura que cumpriu todos os procedimentos indicados acima.

6. Regras quanto ao Registro das Operações

O registro das ordens será feito por meio de sistema informatizado da corretora que for realizada a operação, contendo as seguintes informações:

- Código de identificação dos clientes;
- Data e horário;
- Objeto da Ordem (característica do ativo a ser negociado);
- Natureza da Operação (Compra ou venda e o tipo de mercado);
- Quantidade;
- Preço;
- Identificação do Operador responsável pela operação.

A ordem poderá também ser alterada quando houver um erro operacional. Essas alterações devem ser feitas dentro dos horários estabelecidos pela BOVESPA.

A Finacap pode reespecificar o comitente em operações realizadas exclusivamente para as contas dos Clientes que sejam carteiras e fundos de investimento por ele geridos, que tenham sido previamente cadastradas junto ao intermediário, exclusivamente entre elas.

A Finacap também pode reespecificar operações em que tenha ocorrido erro operacional, desde que este seja devidamente justificado e documentado, nos termos das regras editadas pelas entidades administradoras de mercado organizado.

7. Regras quanto ao cancelamento e reespecificação das ordens

Toda e qualquer ordem enquanto não executada, poderá ser cancelada pela Finacap quando:

- Os dados apontarem risco para o cliente;
- Contrariar as normas operacionais do mercado de valores mobiliários;
- Quando identificados atos ilíticitos notadamente voltadas à criação de condições de preços artificiais, manipulação de preços.

8. Exceções

O rateio não deve ser utilizado nos seguintes casos:

- Enquadramento ativo ou passivo da carteira ou do fundo;
- Indivisibilidade do lote e quantidade negociada muito pequena;
- Restrições individuais de cada fundo ou carteira restringindo operações;
- Ordens de compra e venda com a identificação do Fundo ou Carteira na qual elas devem ser executadas.

9. Responsabilidades

A Finacap não será responsável por prejuízos sofridos pelos Clientes que sejam decorrentes de:

a) variações de preços inerentes às operações realizadas nos mercados à vista e de liquidação futura;

b) atos culposos ou dolosos praticados por terceiros;

c) interrupção do serviço devido à ocorrência de caso fortuito ou força maior, variação brusca de preços e baixa de liquidez no mercado;

d) interrupções nos sistemas de comunicação, oriundos de falhas e/ou intervenções de qualquer prestador de serviços de comunicação, tecnologia ou de outra natureza e, ainda, falhas na disponibilidade e acesso ao sistema de operações ou em sua rede.

Quaisquer prejuízos sofridos pelos Clientes em decorrência das respectivas políticas de investimento são de sua inteira responsabilidade.

10. Comitê de Investimento/Crédito

Este comitê foi criado com a intenção de tornar o processo decisório de investimento mais transparente, eficiente e seguro. É responsável, de forma colegiada, pela discussão das possibilidades de investimento, acompanhamento das atividades dos gestores, acompanhamento da gestão de riscos, promoção de princípios de governança, entre outros. Além disso, o comitê é também é responsável pela auditoria e controle das negociações de ativos por parte dos gestores da Finacap, com as seguintes funções:

- Aprovar propostas de compra de novos ativos, sempre levando em consideração as características explicitas e implícitas dos riscos associados, principalmente para Títulos de Crédito Privado;
- Aprovar estratégias de alocação, sempre ponderando risco e retornos esperados na seleção entre emissões públicas e privadas;
- Regular a exposição aos diferentes fatores de risco das carteiras geridas pela Finacap;
- Avaliar as políticas de rateio e divisão de ordens que tragam equidade a todos os clientes, carteiras e fundos na execução de novas ordens;
- Avaliar risco de crédito associado às possíveis perdas que o credor tenha caso o devedor (contraparte) não honre com os seus compromissos, isto é, a falta de numerário/caixa necessário para o cumprimento de uma ou mais obrigações.

Composição:

O comitê de Investimento é composto por diretores líderes das diretorias de Risco e Compliance, Comercial e de Investimentos e se reúne semanalmente para a discussão de pautas importantes relacionadas à gestão de ativos e riscos. Todas as avaliações e deliberações do Comitê de Investimento são registradas formalmente e em ata própria.

11. Comitê de Risco/Compliance

Este Comitê tem como pauta permanente, discutir, acionar, deliberar, apresentar informações que, direta ou indiretamente, afetem operações ativas e/ou passivas nos recursos sob gestão da FINACAP, prioritariamente nos aspectos de riscos e conformidade aos regulamentos e normas dos órgãos reguladores. Pautas específicas deverão ser antecipadamente propostas às reuniões, ou excepcionalmente durante as mesmas. Cabe ao comitê realizar revisão da metodologia da apuração dos riscos descritos mais abaixo. Os riscos mencionados consistem no grau de incerteza da rentabilidade de um investimento está associado à probabilidade de ganhos ou perdas acima ou abaixo da média do mercado. Os principais riscos envolvidos no negócio podem ser classificados em:

Risco de Mercado: é a possibilidade de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição. Neste caso ligado aos veículos de aplicação geridos pela Finacap ou de sua carteira própria.

Risco de Liquidez: está associado à capacidade de comprar/vender um investimento sem afetar substancialmente o preço, isto é, a falta de contrapartes em número suficiente ou do interesse do mercado em negociar a quantidade desejada de uma posição, afetando de forma anormal o seu preço. Neste caso ligado aos veículos de aplicação geridos pela Finacap ou de sua carteira própria.

Risco Operacional: decorrem da possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação dos sistemas de informação, processamento e operações, bem como, de falhas nos controles internos, fraudes ou qualquer tipo de evento não previsto, que torne impróprio o exercício das atividades da Distribuidora, resultando em perdas inesperadas. Para sua medição e acompanhamento são utilizados os processos e as ocorrências de riscos efetivamente observados de cada departamento da Finacap Consultoria e Mercado de Capitais.

Risco de Compliance: decorre da possibilidade de desvio ou inconformidade que possa ocorrer entre a execução das atividades da Finacap Consultoria e Mercado de Capitais e o

conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para os processos.

Composição: Diretor Risco/Compliance e Diretor Investimento, com reunião semanal.

12. Política de Investimentos Pessoais

O objetivo desta política é regular o investimento em ativos que possam gerar conflitos entre as atividades desempenhadas pelos colaboradores da **FINACAP**, seus clientes e o mercado financeiro, e ainda sem prejuízo do tratamento de confidencialidade das informações, obtidas pelos colaboradores, no exercício das suas respectivas atividades.

Princípios Básicos

- Assegurar tratamento justo e igualitário entre todos os colaboradores;
- Assegurar a realização de investimentos pessoais dentro dos procedimentos legais e de mercado;
- Proteger os interesses dos clientes, acionistas e colaboradores da gestora; e
- Assegurar que as transações dos clientes e/ou dos fundos ocorrem prioritariamente as dos colaboradores.

A presente política abrange e deve ser cumprida integralmente por:

- (i) administradores, empregados, operadores e prepostos da **FINACAP**; (ii) sócios da FINACAP, pessoas físicas; (iii) os sócios e sociedades controladas direta ou indiretamente pela **FINACAP**, pessoas jurídicas; (iv) demais profissionais que mantenham, com a **FINACAP**, contrato de prestação de serviços diretamente relacionados à atividade de gestão; e (v) cônjuges ou companheiros, filhos menores ou quaisquer dependentes financeiramente das pessoas mencionadas nos incisos I, II, III e V acima (“Pessoas Vinculadas”); e
- E demais pessoas que estejam relacionadas direta ou indiretamente com a **FINACAP** nos casos em que houver exigência legal ou regulamentar ou por decisão do Comitê de Risco e *Compliance*.

Esta Política de Investimentos Pessoais exprime parte das metas e princípios de ética que norteiam os negócios da **FINACAP** e são complementares aos demais manuais de política internos e às leis e normativos aplicáveis pelos reguladores. O desrespeito a presente Política será considerado infração contratual, sujeitando seu autor às penalidades cabíveis, nos termos da legislação aplicável.

Regras

As Pessoas Vinculadas e demais pessoas subordinadas a presente Política devem observar as seguintes regras:

- Respeitar à integridade dos mercados;
- Não realizar operações que possam prejudicar o bom andamento dos mercados;
- Não girar de carteiras de forma excessiva, manipular preços e/ou forjar demanda por papéis, criar ou incentivar rumores, criar demandas artificiais de mercado; realizar ofertas de valores mobiliários;
- Não realizar operações com o objetivo de promover acertos entre contrapartes, ou quaisquer operações de natureza artificial, simulação ou que não estejam de acordo com os usos e costumes e as boas práticas de mercado;
- Não se envolver em situações que gerem situações artificiais ou de manipulação do mercado ou das carteiras sob gestão da **FINACAP**;
- Profissionalismo e respeito aos limites impostos pela **FINACAP**;
- Não realizar quaisquer atividades em situação de conflito de interesses com a **FINACAP**; e
- Não utilizar as informações confidenciais obtidas em função de suas atividades na **FINACAP** para obter vantagem pessoal ou para terceiros.

A **FINACAP** poderá, a qualquer momento, criar listas de restrição à negociação, vedar a utilização de certas estratégias ou o investimento em certas classes de ativos, seja por

entender que tais iniciativas podem comprometer os princípios gerais aqui descritos, seja pelo perfil de risco que entende ser adequado aos seus colaboradores.

A presente Política tem como base a responsabilidade pessoal e o comprometimento ético dos colaboradores da **FINACAP**. Os atos que tenham por objetivo burlar as regras aqui previstas, bem como aquelas previstas na legislação aplicável, são consideradas faltas graves e serão remetidas ao Comitê de Risco e *Compliance,* que irá definir eventuais sanções aplicáveis.

É VEDADA a prática de *Insider Trading*, divulgação de informação privilegiada a terceiros e *Front Running* por qualquer colaborador da FINACAP, seja para uso em benefício próprio, da FINACAP ou de terceiros. Entende-se por *Insider Trading* e *Front Running*:

- *Insider Trading* consiste na compra e venda de títulos ou valores mobiliários ou não mobiliários com base na utilização de informação privilegiada, visando à obtenção de benefício próprio ou de terceiros (incluindo a própria **FINACAP** e demais Pessoas Vinculadas);

- Divulgação de Informação Privilegiada é a divulgação, a qualquer terceiro, de informação privilegiada que possa ser utilizada com vantagem na compra e venda de títulos ou valores mobiliários; e

- *Front Running* é a prática de se aproveitar alguma informação privilegiada para concluir uma negociação antes de outros, principalmente de clientes da **FINACAP**.

A utilização ou divulgação de informação privilegiada, *Insider Trading* e *Front Running* sujeitará os responsáveis às sanções, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da **FINACAP**, ou demissão por justa causa, sem prejuízo das medidas legais cabíveis.

Quaisquer dúvidas em relação à interpretação desta Política de Investimentos Pessoais devem ser imediatamente informadas ao coordenador do Comitê de Risco e Compliance para que sejam sanadas previamente à realização de quaisquer investimentos pessoais pelos Colaboradores que possam configurar a posteriori desrespeito ao espírito

desta norma. Seu desconhecimento não mitiga a aplicação de sanções pelo Comitê de Risco e Compliance da **FINACAP**.

MANUAL DE PREVENÇÃO À LAVAGEM DE DINHEIRO E OCULTAÇÃO DE BENS

1. Caracterização Legal

A Lei nº 9.613/98, no seu artigo 1º, tipifica o crime de lavagem como: “Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos e valores provenientes, direta ou indiretamente, de infração penal”.

2. Obrigações

A Finacap Consultoria Financeira e Mercado de Capitais, no âmbito de suas atividades, deve indicar à Comissão de Valores Mobiliários (CVM) e ao Banco Central do Brasil (BACEN), um diretor responsável pelo cumprimento das obrigações estabelecidas pela legislação e para assinatura de toda e qualquer comunicação relacionada ao assunto.

A Finacap Consultoria Financeira e Mercado de Capitais cadastra seus clientes e mantêm seus cadastros, documentos e dados devidamente preenchidos e atualizados, e os mantém arquivados pelo prazo de 5 (cinco) anos, mesmo após o encerramento da conta.

Além das informações cadastrais, requeridas quando do cadastramento, constam no cadastro dados relativos à capacidade econômica e rendimentos do cliente.

A Finacap Consultoria Financeira e Mercado de Capitais mantém registro de todas as operações realizadas pelos seus clientes, continuando com os mesmos arquivados pelo prazo de 5 (cinco) anos, após a data da conclusão da operação.

3. Limite Operacional do Cliente / Cadastro

O limite operacional do cadastro é baseado nos valores informados pelo cliente em sua ficha cadastral e declarações que eventualmente poderão ser solicitadas. Os parâmetros utilizados são os seguintes:

a. Pessoa Física até o limite de:

Renda Mensal	80%
Bens Líquidos (Renda Fixa, Renda Variável, Depósitos à Vista, Poupança, etc)	70%
Bens Ilíquidos (Imóveis, Móveis, Obras de Arte, Participações Societárias, etc)	40%
Valor Líquido dos Ativos Aplicados na Finacap (em relação ao mês anterior)	100%

b. Pessoa Jurídica até o limite de:

Patrimônio Líquido	70%
Valor Líquido dos Ativos Aplicados na Finacap (em relação ao mês anterior)	100%

Além dos limites operacionais estipulados para o cliente pessoa jurídica será levada em consideração a sua capacidade financeira através de análise das demonstrações

contábeis como: balanço patrimonial, demonstrativo de resultados e seu fluxo de caixa (todos necessariamente auditados).

Para menores de 18 anos ou clientes sem renda mensal e/ou patrimônio declarado, pode-se considerar como limite operacional os percentuais abaixo aplicados sobre o limite operacional de seus responsáveis definidos no cadastro.

Até o limite de:

Renda Mensal	20%
Bens Líquidos	10%
Bens Ilíquidos	7%
Valor Líquido dos Ativos Aplicados na Finacap em seu nome (em relação ao mês anterior)	100%

4. Indício de Ocorrência de Crime

A Finacap Consultoria Financeira e Mercado de Capitais dispensará relevante atenção no cadastramento de clientes, na proposição de operações e na realização das mesmas, a fim de verificar indícios de crime ou suspeitas de atividades ilícitas, nas seguintes situações:

• Operações cujos valores sejam objetivamente incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial/financeira de quaisquer das partes envolvidas, tomando-se por base as informações cadastrais;

• Operações que evidenciem oscilação significativa em relação ao volume e/ou frequência de negócios de quaisquer das partes envolvidas;

• Operações cujos desdobramentos contemplem características que possam constituir artifício para burla da identificação dos efetivos envolvidos e/ou beneficiários respectivos;

• Operações cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;

• Operações que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelos envolvidos;

• Operações com clientes oriundos de cidades fronteiriças;

• Operações com clientes não-residentes, avaliando se o seu país de origem não vem a ser um dos países classificados como paraíso fiscal pela Receita Federal ou que não cumprem as recomendações do GAFI;

• Operações com clientes Pessoa Politicamente Exposta de nacionalidade brasileira ou nacionalidade que se enquadre no item anterior; e

• Situações que não seja possível atualizar as informações cadastrais do cliente.

5. Comunicação

A Finacap Consultoria Financeira e Mercado de Capitais comunicará ao COAF, no prazo de 24 (vinte e quatro horas) após a efetiva análise da documentação, qualquer proposta ou realização de operações em que se constatem indícios de lavagem de dinheiro, tais como:

• Operações em espécie com montantes superiores a R$ 50.000,00 que possam configurar a existência de indícios dos crimes previstos na Lei 9.613/98;

• Operações cujo titular da ordem ou beneficiário final sejam as entidades, pessoas físicas ou jurídicas descritas na Carta Circular 3.342/08 e nos Comunicados 17.351/08 e 17.328/08; e

• Outras operações que possam configurar a existência de indícios dos crimes previstos na Lei 9.613/98, conforme a Carta Circular 3.542/12, do Banco Central.

6. Responsabilidade Administrativa

A Finacap Consultoria Financeira e Mercado de Capitais, bem como seus administradores responsáveis, estão cientes das sanções a que estão sujeitos se deixarem de cumprir as obrigações previstas na Lei 9.613/98 e alterações posteriores.

7. Informação ao Cliente

A Finacap Consultoria Financeira e Mercado de Capitais, conforme impõe a legislação em vigor, abstém-se de fornecer aos clientes informações sobre eventuais comunicações efetuadas em decorrência de indícios de crime de “lavagem”.

8. Documentação

A Finacap Consultoria Financeira e Mercado de Capitais manterá sob guarda os documentos de avaliação da capacidade financeira ou registros de ocorrências que apontarem indícios de crime de "lavagem" ou ocultação de bens, direitos e valores.

A Finacap Consultoria Financeira e Mercado de Capitais deve manter, à disposição do Banco Central e da CVM, no mínimo, por prazo de 5 (cinco) anos, contados do 1º dia útil do ano subsequente ao do encerramento da conta ou da ocorrência, toda documentação correspondente – dados cadastrais dos envolvidos e registro das operações e das ocorrências, nos termos do disposto no artigo 10, § 2º, da Lei 9.613/98, artigo 11 da Circular 3.461/09 e artigo 5 da ICVM 463/08 e alterações posteriores.

9. Política de Prevenção à Lavagem de Dinheiro

Considerando as disposições da Convenção das Nações Unidas contra os Crimes de “Lavagem" e ou Ocultação de Bens, Direitos e Valores, assinada em Viena, Áustria, em 1988 e vigente 1990, Finacap Consultoria Financeira e Mercado de Capitais adotará todas as medidas cabíveis, definidas em Lei e pelos órgãos competentes brasileiros, para a prevenção e combate a esses crimes.

A Finacap Consultoria Financeira e Mercado de Capitais efetiva os controles voltados à prevenção e combate aos crimes de “lavagem” de dinheiro com base nas disposições da Lei nº 9.613/98, e alterações posteriores, e nas normas que a regulamentam.

O objetivo da política é padronizar e direcionar os esforços com vistas à prevenção e ao combate aos crimes de “lavagem” de dinheiro, minimizando, assim, os riscos que tais ilícitos venham a ocorrer na Instituição.

Assim procura definir e implementar:

A) Estrutura organizacional responsável pelo atendimento das disposições contidas nos artigos 10 e 11 da Lei 9.613/98, que dispõe sobre Crimes de “Lavagem” e ou Ocultação de Bens, Direitos e Valores;

B) Critérios relativos à identificação, registro e comunicação de operações ou propostas, cujas características, no que se referem às partes envolvidas, valores, formas de realização e/ou instrumentos utilizados, ou que, pela falta de fundamento econômico ou legal, possam indicar a existência objetiva de indícios de crimes de “lavagem” e ou ocultação de bens, direitos e valores, ou com eles relacionados. E, na identificação de transações suspeitas, proceder a comunicação às autoridades competentes.

C) Conscientização dos funcionários sobre a importância do tema no sentido de mitigar os riscos operacionais envolvidos e o do cumprimento da legislação vigente.

10. Diretoria de Compliance

A Finacap Consultoria Financeira e Mercado de Capitais indicará a Comissão de Valores Mobiliários nos termos da ICVM 558/15, um Diretor responsável pelo cumprimento das obrigações contidas na Lei 9.613/98, e nos demais normativos pertinentes editados pelas referidas autarquias, e pela assinatura de toda e qualquer comunicação relacionada ao assunto; e também será o responsável pela aprovação das políticas, diretrizes e procedimentos para o cumprimento do disposto na legislação sobre crimes de “lavagem” e ou ocultação de bens, direitos e valores.

Ficará a cargo do Diretor responsável a implementação e acompanhamento do cumprimento das medidas estabelecidas para identificar operações suspeitas e cuidar do registro e da manutenção de dados e documentos das operações, ou propostas, que

apresentem sérios indícios de crimes de “lavagem” e ou ocultação de bens, direitos e valores, podendo, para tanto, designar colaboradores para assisti-lo quanto:

- Análise dos casos de indícios de crimes de “lavagem”, solicitando as áreas internas, esclarecimentos e documentos, estabelecendo prazos de respostas, baseados nos níveis de responsabilidade e risco visando ter documentação e dados suficientes (movimentações financeiras, detecção de operações suspeitas, cadastro de cliente, etc), para encaminhamento das informações ao Comitê de Riscos;
- Após análise das ocorrências pelo Comitê de Riscos e decisão por parte dos membros da necessidade de comunicação aos órgãos competentes ou encaminhamento para arquivamento, elaborar relatório que deverá ser arquivado para que sejam consultados, se necessário, e para que se possa ter um controle efetivo das inconformidades.
- O Comitê também poderá decidir por: sugerir a renovação ou não da ficha cadastral, promover visita ao cliente ou, ainda, re-analisar a situação financeiro-patrimonial do cliente.

O Comitê de Investimento e Riscos da Finacap Consultoria Financeira e Mercado de Capitais, que se reúne periodicamente, apreciará e deliberará sobre as questões que envolvam a prevenção e combate aos crimes de “lavagem” de dinheiro. Essas deliberações serão registradas em atas e mantidas em arquivo próprio.

11. Responsabilidades das Áreas e dos Funcionários

Todos os colaboradores devem observar o cumprimento da política de prevenção à lavagem de dinheiro e, ao detectarem ou tomarem conhecimento de uma operação ou receberem proposta de operação atípica ou suspeita de prática de atividades ilícitas de “lavagem” de dinheiro, deverão comunicar a diretoria responsável.

A comunicação deverá ser por escrito relatando as suspeitas, denúncias ou indícios de crimes de “lavagem” e ou ocultação de bens, direitos e valores.

12. Política Conheça seu Cliente – Know Your Client / KYC

A identificação do cliente deve ser satisfatoriamente estabelecida antes de iniciar qualquer relacionamento. As orientações sobre o preenchimento e documentação dos dados cadastrais dos clientes estão definidas nos processos de cadastro de pessoas físicas e jurídicas pertencentes ao “Descrição de Processos KYC”.

Sempre que possível deve-se dar preferência a visita pessoal do cliente à Finacap Consultoria Financeira e Mercado de Capitais para o preenchimento de sua ficha cadastral. Caso isso não seja possível é importante que o analista procure fazer uma avaliação mesmo que sintética da forma de conduta do cliente e assinalar atitudes que lhe pareçam distintas da normalidade respeitando a individualidade de cada cliente.

13. Política Conheça seu Funcionário

Cabe a Diretoria Administrativa e *Compliance* estabelecer política que contemple o acompanhamento do funcionário, desde os procedimentos de admissão, seu desenvolvimento dentro da empresa, até o seu desligamento, mantendo-o permanentemente atualizado. As operações realizadas pelos colaboradores na Distribuidora deverão ser acompanhadas e estar de acordo com as regras vigentes para operações de pessoas vinculadas.

O processo de integração de novos colaboradores é realizado através de uma apresentação que tem por objetivo principal apresentar a história, a estrutura da empresa, sua missão, princípios e suas principais políticas e atribuições de cada setor.

Além disso, devem ser entregues os Manuais do Sistema de Controles Internos e de Segurança de TI e o Código de Conduta e Ética e assinados os seus respectivos termos de adesão.

14. Treinamento sobre Prevenção Contra Crimes de "Lavagem" e ou Ocultação de Bens, Direitos e Valores

A Diretoria Administrativa e *Compliance* deve elaborar a programação de treinamentos sobre Prevenção à “Lavagem” de Dinheiro – PLD, objetivando atender o disposto no artigo 1 inciso III da Circular 3.461/09 e artigo 9 – item 2 da ICVM 463/08. Além disso, efetuar o controle dos colaboradores que foram treinados ou deverão ser.

15. Auditorias Interna e Externa

As auditorias interna e externa em seus trabalhos regulares deverão avaliar a adequação das rotinas à legislação vigente e dar parecer mediante testes e exames sobre a efetividade destas rotinas no sentido de detecção de lavagem de dinheiro, e análise de operações suspeitas.

16. Caracterização dos Crimes de Lavagem de Dinheiro

A “Lavagem” de Dinheiro é o processo pelo qual o criminoso transforma recursos ganhos em atividades ilícitas em ativos com uma origem aparentemente legal.

Essa prática geralmente envolve múltiplas transações, usadas para ocultar a origem dos ativos financeiros e permitir que eles sejam utilizados sem comprometer os criminosos. A dissimulação é, portanto, a base para toda operação de “lavagem” de dinheiro proveniente de um crime antecedente.

17. Instrumentos Internacionais de Cooperação

O tema Crimes de "Lavagem" de Dinheiro, embora conhecido desde a década de 80, difundiu-se, nos últimos anos, em conferências internacionais e a preocupação com os aspectos práticos do combate a esse crime começou a se materializar de forma mais ampla já no início dos anos 90. Desde então, diversos países têm tipificado o crime e criado agências

governamentais responsáveis pelo combate à "lavagem" de dinheiro. Essas agências são conhecidas mundialmente como *FIU - Financial Intelligence Unit* ou Unidades Financeiras de Inteligência.

18. Criação da UIF / COAF do Brasil

A resposta brasileira ao problema veio com a promulgação da Lei 9.613/98 – que dispõe sobre os Crimes de "Lavagem" e ou Ocultação de Bens, Direitos e Valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; e criou o Conselho de Controle de Atividades Financeiras - COAF, entre outras providências.

• Conselho de Controle de Atividades Financeiras – COAF: de acordo com o artigo 14 da Lei 9.613/98, o COAF tem a finalidade de (i) disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas na Lei, sem prejuízo da competência de outros órgãos e entidades; e coordenar e propor mecanismos de cooperação e de troca de informações que viabilizem ações rápidas e eficientes no combate à ocultação ou dissimulação de bens, direitos e valores.

Esses procedimentos, basicamente, implicam a obrigatoriedade pelos agentes econômicos de identificar clientes e manter cadastros atualizados, registrar todas as transações acima de determinado limite e de comunicar as operações suspeitas aos órgãos competentes.

19. Efeitos da Condenação pela Prática de Crime de “Lavagem” de Dinheiro

Conforme previsto na referida Lei, se condenadas, as pessoas físicas sofrerão as seguintes sanções:

Art. 7. São efeitos da condenação, além dos previstos no Código Penal:

I - Perda, em favor da União - e dos Estados, nos casos de competência da Justiça Estadual -, de todos os bens, direitos e valores relacionados, direta ou indiretamente, à prática

dos crimes previstos nesta Lei, inclusive aqueles utilizados para prestar a fiança, ressalvado o direito do lesado ou de terceiro de boa-fé; (Redação dada pela Lei 12.683/12)

II - Interdição do exercício de cargo ou função pública de qualquer natureza e de diretor, de membro de conselho de administração ou de gerência das pessoas jurídicas referidas no art. 9, pelo dobro do tempo da pena privativa de liberdade aplicada.

20. Deveres de Identificação e de Comunicação

A Lei 9.613/98 e diversos normativos emanados das autoridades competentes obrigam as instituições financeiras e outras instituições e empresas a adotarem medidas efetivas com vistas à prevenção à “lavagem” de dinheiro - identificar clientes e manter cadastros atualizados, registrar todas as transações acima de determinado limite e de comunicar as operações suspeitas aos órgãos competentes - sob pena de ser-lhes aplicadas às sanções previstas em seu artigo 12, que assim dispõe:

Art. 12. Às pessoas referidas no art. 9, bem como aos administradores das pessoas jurídicas, que deixem de cumprir as obrigações previstas nos arts. 10 e 11 serão aplicadas, cumulativamente ou não, pelas autoridades competentes, as seguintes sanções:

I - advertência;

II - multa pecuniária variável não superior:

a) ao dobro do valor da operação;

b) ao dobro do lucro real obtido ou que presumivelmente seria obtido pela realização da operação; ou

c) ao valor de R$ 20.000.000,00 (vinte milhões de reais);

III - inabilitação temporária, pelo prazo de até dez anos, para o exercício do cargo de administrador das pessoas jurídicas referidas no art. 9º;

IV - cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento.

§ 1º A pena de advertência será aplicada por irregularidade no cumprimento das instruções referidas nos incisos I e II do art. 10.

§ 2o A multa será aplicada sempre que as pessoas referidas no art. 9o, por culpa ou dolo:

I – deixarem de sanar as irregularidades objeto de advertência, no prazo assinalado pela autoridade competente;

II - não cumprirem o disposto nos incisos I a IV do art. 10;

III - deixarem de atender, no prazo estabelecido, a requisição formulada nos termos do inciso V do art.10;

IV - descumprirem a vedação ou deixarem de fazer a comunicação a que se refere o art. 11.

§ 3º A inabilitação temporária será aplicada quando forem verificadas infrações graves quanto ao cumprimento das obrigações constantes desta Lei ou quando ocorrer reincidência específica, devidamente caracterizada em transgressões anteriormente punidas com multa.

§ 4º A cassação da autorização será aplicada nos casos de reincidência específica de infrações anteriormente punidas com a pena prevista no inciso III do caput deste artigo.

21. Salvaguarda Legal

Nos termos do disposto no artigo 11, § 2º, da Lei 9.613/98, as comunicações feitas de boa-fé não acarretarão responsabilidade civil e nem administrativa.

22. Legislações Específicas Relevantes

1. Legislação Federal

- Lei nº 9.613/98 - dispõe sobre os crimes de "lavagem" e ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; e cria o Conselho de Controle de Atividades Financeiras – COAF.
- Lei Complementar 105/01 - dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.

2. Banco Central do Brasil – BCB

- Carta Circular 3.542/12 - divulga relação de operações e situações que podem configurar indícios de ocorrência dos crimes previstos na Lei 9.613/98 passíveis de comunicação ao Conselho de Controle de Atividades Financeiras (Coaf).
- Circular 3461/09 - consolida as regras sobre os procedimentos a serem adotados na prevenção e combate às atividades relacionadas com os crimes previstos na Lei nº 9.613/98.
- Carta Circular 3.342/08 - dispõe sobre a comunicação de movimentações financeiras ligadas ao terrorismo e ao seu financiamento.
- Carta Circular 3.151/04 - divulga instruções para as comunicações previstas no art. 4 da Circular 2.852/98, e na Carta-Circular 3.098/03.
- Carta Circular 3.098/03 - esclarece sobre o registro de depósitos e retiradas em espécie, bem como de pedidos de provisionamento para saques.
- Circular 3.030/01 - dispõe sobre a identificação e o registro de operações de depósitos em cheque e de liquidação de cheques depositados em outra instituição financeira, bem como de emissões de instrumentos de transferência de recursos.
- Carta Circular 3.430/10 - esclarece aspectos relacionados à prevenção e combate às atividades relacionadas com os crimes previstos na Lei nº 9.613/98, tratados na Circular 3.461/09.
- Circular 3.570/11 - estabelece a obrigatoriedade de prestação de informações relacionadas às Resoluções do Conselho de Segurança das Nações Unidas (CSNU) incorporadas ao ordenamento jurídico brasileiro, promove alterações no Regulamento do Mercado de Câmbio e Capitais Internacionais (RMCCI) e dá outras providências.
- Circular 3.583/12 - altera a Circular 3.461/09, que consolida as regras sobre os procedimentos a serem adotados na prevenção e combate às atividades relacionadas com os crimes previstos na Lei 9.613/98.

3. Superintendência de Seguros Privados - SUSEP

- Circulares SUSEP 327/06 - dispõem sobre os controles internos específicos para o tratamento de situações relacionadas à prática dos crimes previstos na Lei nº 9.613/98, ou que com eles possam se relacionar, a comunicação de operações suspeitas e a responsabilidade administrativa de que trata aquela Lei.

4. Comissão de Valores Mobiliários - CVM

- Instrução CVM 301/99 - dispõe sobre a identificação, o cadastro, o registro, as operações, a comunicação, os limites e a responsabilidade administrativa de que tratam os incisos I e II do art. 10, I e II do art. 11, e os artigos 12 e 13 da Lei 9.613/98, referente aos crimes de "lavagem" ou ocultação de bens, direitos e valores.
- Instrução CVM 463/08 - altera a ICVM 301/99, e dispõe acerca dos procedimentos a serem observados para o acompanhamento de operações realizadas por pessoas politicamente expostas – PPE's. Tem como principais destaques: acompanhamento mais cuidadoso do relacionamento com pessoas politicamente expostas; ampliação do rol de hipóteses de comunicação de "operações suspeitas"; estabelecimento de procedimentos cadastrais diferenciados para os chamados clientes de alto risco e procedimentos de controle interno e programas de treinamento de funcionários sobre as exigências da Instrução.
- Instrução CVM 505/11 - estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.
- Instrução CVM 506/11 - altera a ICVM 301/99. Revoga o art. 12 da ICVM 14/80.
- Instrução CVM 523/12 - altera artigos da ICVM 301/99.

5. Conselho de Controle de Atividades Financeiras - COAF

- O COAF – Conselho de Controle de Atividades Financeiras disponibiliza em seu site - www.fazenda.gov.br/coaf - resoluções para as instituições não fiscalizadas pelo Banco Central, CVM, Susep e Previdência Complementar. Destacam-se entre elas: compra e venda de imóveis; *factoring*; loterias e sorteios; jóias e metais preciosos; jogos de bingo; administradoras de cartões de crédito ou credenciamento; bolsas de mercadorias e corretores; objetos de arte e antiguidades.

23. Atribuições do Comitê de Riscos

Compete ao Comitê de Riscos deliberar sobre:

1. Casos suspeitos de "lavagem" submetidos pela diretoria responsável e definir sobre sua comunicação ao COAF;

2. As propostas de encerramento de relacionamento com clientes que tiveram seus nomes envolvidos em comunicação ao COAF;

3. Caso o cliente seja suspeito de crime de lavagem o seu nome será encaminhado ao Banco Central e CVM, conforme determina a legislação;

4. Arquivamento dos demais casos.

Toda decisão do Comitê deverá ser tomada por consenso entre os seus membros, lavrado em ata. Cabe ao Comitê analisar e aprovar os novos produtos e serviços que a distribuidora vier a desenvolver sob a ótica da prevenção dos crimes de lavagem ou ocultação de bens. Somente após a aprovação pelo comitê os novos produtos poderão ser distribuídos pela corretora.

MANUAL DE SUITABILITY

Objetivo

A presente política tem por objetivo prover direcionamento e padronização para o processo de identificação do perfil de riscos dos investidores, a recomendação de produtos Fundos de Investimentos, bem como a adequação de tais produtos ao perfil do Investidor.

Esta política se enquadra nos padrões estabelecidos pelas regulamentações e normas abaixo:

- Instruções CVM nº539/13, 555/14, 409/04 e 555/14

- Código Anbima de Melhores Práticas para Fundos de Investimento

- Código de Ética e Conduta da Finacap Consultoria Financeira e Mercado de Capitais LTDA

1. Abrangência

Aplicável a todos os colaboradores da Finacap Consultoria Financeira e Mercado de Capitais LTDA que têm relacionamento com clientes e principalmente os que atuam diretamente na captação de recursos para investimento em produtos da Finacap Consultoria Financeira e Mercado de Capitais LTDA.

2. Processo de Suitability

2.1. Metodologia

2.1.1. Cotista

Para ingresso do investidor é preciso que seja mensurado seu perfil (Suitability) de risco, através do questionário para identificação de perfil do investidor. Existem 2 questionários, Pessoa Física e Pessoa Jurídica, que são parte integrante das fichas cadastrais e que são reavaliados a cada 2 anos. A reavaliação do perfil poderá ser feita a qualquer momento também, substituindo o questionário anterior.

Clientes que não tenham o perfil de investidor definido não poderão aplicar no fundo ou carteira administrada. Entretanto, caso o cliente ordene a realização da aplicação, esta poderá ser acatada mediante assinatura do termo específico (TCQ – Termo de Ciência de Questionário); este termo se aplica somente ao primeiro investimento no fundo feito pelo cotista e não possui prazo de validade, permanecendo válido até o resgate total das cotas.

Após o resgate total do investimento e quando houver nova aplicação, um novo termo deverá ser assinado.

2.1.2. Produto

Para definir os fatores de risco de um produto são levados em consideração os riscos de: crédito, mercado, liquidez, operacional.

O processo de suitability utiliza a visão produto, ou seja, a adequação aos investimentos irá contemplar o risco isolado de cada investimento.

2.1.3. Processo

As etapas do processo de Suitability que fazem parte do processo de identificação do perfil de risco do investidor estão contidas nesta política.

As etapas do processo de Suitability:

1) Cadastro de acordo com a ICVM 301;
2) Chegagem de Informações Públicas;
3) Formulário Suitability;
4) Aplicação via CETIP/TED/DOC;
5) Monitoramento das Movimentações, Lei 9.613.

Com relação ao suitability, caso o cliente não esteja com o perfil de investidor de acordo com a aplicação, sera necessário o mesmo assinar um termo de ciência e risco.

2.2. Enquadramento e Desenquadramento

O Perfil estará enquadrado quando a pontuação atingida for maior ou igual à pontuação exigida para o produto em questão a cada nova aplicação. O desenquadramento pode ocorrer em 2 situações distintas e são classificados como: ativo e passivo.

2.2.1. Desenquadramento Ativo

O investidor devidamente aprovado em comitê que desejar aplicar em fundo em discordância com o seu perfil de risco deve assinar o termo de ciência de desenquadramento.

2.2.2. Desenquadramento Passivo

Em posterior análise, após o momento da aplicação, o perfil de risco do investidor e o produto não mais correspondem e o investidor está desenquadrado passivamente.

Para corrigir a situação de desenquadramento passivo existem 3 opções:

- Solicitar resgate
- Assinar termo de ciência de desenquadramento
- Atualizar o perfil através de aplicação de novo questionário.

O TCD assinado pelo investidor vale enquanto ele mantiver o investimento no fundo. Caso aconteça o resgate total e o cliente manifeste intenção de aplicar novamente, um novo TCD será assinado.

3. REGRA PARA OFERTA DE PRODUTOS

De acordo com os perfis de risco para investidores especificados nos questionários de Suitability alguns produtos podem ter restrição ou vedação ao tipo de investidor.

Ainda que neste momento alguns tipos de fundo não sejam ofertados pela Finacap Consultoria Financeira e Mercado de Capitais LTDA, valem as qualificações a seguir.

Obs.: a regra vale para a compra direta do produto de investimento, e não para aquela feita através de fundo de investimento da casa (desde que o fundo mantenha-se devidamente enquadrado na regulamentação vigente).

'Restritos' são produtos nos quais os clientes podem investir, mas por iniciativa própria. A área de distribuição não pode oferecer um produto restrito a uma categoria de investidor, caso o produto não seja adequado àquele perfil de risco.

'Vedado' é o tipo de investimento no qual, mesmo o cliente demonstrando interesse pelo mesmo, não poderá investir; nem mesmo por iniciativa própria.

4. COMUNICAÇÃO DE CLIENTES

Clientes sem Perfil de Investidor definido ou com Perfil de Investidor desatualizado não podem ser destinatários de comunicação que se caracterize como recomendação de investimento.

5. MODELO OPERACIONAL

5.1. Cadastro do Perfil de Investidor

O responsável pelo cadastro, incluindo a cobrança do preenchimento dos questionários pelo cliente, é o próprio responsável comercial pelo cliente. O setor administrativo faz em seguida um double-check.

5.1.1. Validação do Perfil do Investidor

Posteriormente à identificação do Perfil do Investidor, sempre que possível, será feita avaliação histórica dos investimentos do cliente, de modo a validar (ou não) o Perfil do Investidor declarado, eventualmente atualizando-o com novo preenchimento/assinatura de questionários e atualização de cadastro.

5.2. Tratamento dos Desenquadramentos

Nos casos em que houver desenquadramento, cabe também ao responsável pelo cliente atualizar seu cadastro com novo preenchimento/assinatura de questionários, informando o novo Perfil de Investidor, assim como solicitar toda a documentação pertinente, para que o investimento seja efetivado/mantido.

Para os casos em que o cliente desejar aplicar em produtos ‘vedados’ pelo Perfil do Investidor, a ordem não será efetivada enquanto não houver alteração do mesmo, adequando-se ao risco incremental do investimento.

ANEXO I – QUESTIONÁRIO PESSOA FÍSICA

IDENTIFICAÇÃO DO PERFIL DO INVESTIDOR (SUITABILITY)

Nome do Cotista Titular:
CPF do Cotista Titular:
Data:

- Seção 1

Responda às questões abaixo escolhendo a alternativa que melhor se adequa a seu perfil, tendo em vista sua situação financeira, seus objetivos e sua tolerância a riscos. Assinale apenas uma alternativa em cada questão. Responda a todas às questões.

PARA USO DO DISTRIBUIDOR (Pontos de cada resposta)

1. Como você se comporta em relação aos seus investimentos?

a. Quero evitar perder qualquer parcela dos meus investimentos no horizonte de 3 meses, mesmo que limite os meus ganhos às taxas básicas de juros. [0 ponto]

b. Quero evitar perder qualquer parcela dos meus investimentos no horizonte de 1 ano, mesmo que tenha ganhos menores. [20 pontos]

c. Posso aceitar pequenas perdas em busca de ganhos maiores no longo prazo. [50 pontos]

d. Posso aceitar perdas maiores em busca de ganhos muito elevados. [100 pontos]

2. Suponha que em um dia de crise suas aplicações financeiras desvalorizaram 10%. O que você faria?

a. Resgataria imediatamente meus investimentos para evitar mais perdas. [0 ponto]

b. Avaliaria se a queda criou oportunidades no mercado e eventualmente compraria os ativos desvalorizados. [40 pontos]

c. Observaria por mais algum tempo e, se as perdas continuassem, resgataria meus investimentos. [20 pontos]

3. Como você definiria o seu momento de vida?

a. Etapa de construção do meu patrimônio, não tenho grandes compromissos financeiros e posso guardar renda. [30 pontos]

b. Tenho parte da minha renda comprometida com despesas fixas e continuo com crescimento de meu patrimônio. [20 pontos]

c. Construí um patrimônio considerável, estou realizando meus objetivos, mas ainda mantenho despesas elevadas. [10 pontos]

d. Patrimônio consolidado que considero suficiente para preservação do meu estilo de vida e usufruir. [0 ponto]

4. Existe alguma previsão para utilização dos recursos dos seus investimentos no curto ou médio prazo?

a. Existe previsão de utilização de parte importante ou da integralidade dos recursos em até 1 ano [0 ponto]

b. Existe previsão de utilização de parte importante ou da integralidade dos recursos em até 5 anos. [30 pontos]

c. Não há nenhuma previsão de utilização de parte relevante dos recursos no curto ou médio prazo. [70 pontos]

5. Com quais investimentos você tem familiaridade, pensando no funcionamento e riscos de cada um? Leve em consideração, além da sua experiência com os investimentos, sua formação acadêmica e experiência profissional.

a. Poupança, CDB ou fundos DI. [0 ponto]

b. Além dos anteriores, outros produtos de Renda Fixa (atrelados à inflação e títulos pré- fixados) ou fundos multimercados. [10 pontos]

c. Além de qualquer um dos itens mencionados nas respostas anteriores, ações e fundos de ações. [40 pontos]

d. Além de qualquer um dos itens mencionados nas respostas anteriores, também conheço derivativos. [50 pontos]

e. Além de qualquer um dos itens mencionados nas respostas anteriores, produtos ilíquidos como Private Equity e Fundos Imobiliários de Incorporação. [70 pontos]

TOTAL DE PONTOS (SOMATÓRIO DOS PONTOS OBTIDOS NAS 5 QUESTÕES)

A partir do somatório de pontos, o perfil de investimento sugerido é:

- Seção 2 DECLARAÇÃO

I. Eu concordo com esta definição de perfil.

II. Eu não concordo com esta definição de perfil e explicitamente requisito que o meu perfil seja reclassificado para_____, mesmo que este não seja o mais adequado de acordo com o resultado das respostas do questionário.

NOTA: Se fizer a alteração de perfil, os investimentos poderão ter um nível de risco superior àquele que você afirmou estar disposto a correr com base nas questões acima. É importante saber se essa mudança é, de fato, adequada para você. Por isso, pedimos que responda às perguntas da seção 3.

- Seção 3

6. Aumentar o nível de risco significa aumentar a possibilidade de perdas, não apenas do rendimento dos seus investimentos, mas também de parte do valor investido inicialmente. Você se sente confortável com isso?

a. Sim [10 pontos] b. Não [0 ponto]

7. Você já passou por algum momento de crise em que viu seus investimentos se desvalorizarem significativamente?

a. Já passei por isso, busquei mais informações para analisar a situação e só então tomei uma decisão. [40 ponto]

b. Já passei por isso e resgatei imediatamente meus investimentos para evitar maiores perdas [20 pontos]

c. Nunca passei por isso. [0 ponto]

- Seção 4

Perfil Conservador: busca preservação de capital com baixa tolerância a risco, entendendo que retornos próximos às taxas nominais de juros são suficientes para atingir o objetivo do investimento. Os recursos são preponderantemente alocados em ativos líquidos atrelados às taxas de juros, com alta disponibilidade para necessidades de liquidez. Há, em geral, pouca experiência de investimento em diferentes classes de ativos.

Faixa de Pontuação: até 49 pontos.

Perfil Moderado: busca preservação de capital com objetivo de superar ligeiramente o retorno das taxas nominais de juros. Mantém alguma alocação em ativos de risco, admitindo perdas de patrimônio em situações adversas de mercado. Investe, no entanto, boa parte dos recursos em ativos de baixo risco, buscando retornos acima da inflação no médio prazo e

disponibilizar recursos para eventuais necessidades de liquidez. Há, em geral, alguma experiência de investimento em diferentes classes de ativos.

Faixa de Pontuação: de 50 a 169 pontos.

Perfil Arrojado: busca crescimento elevado de capital com tolerância a risco e baixa necessidade de liquidez. Entende que os ganhos e perdas são inerentes a alocações preponderantemente em ativos de risco, aceitando perdas significativas de patrimônio na busca de maiores retornos no médio ou longo prazo. Há, em geral, boa experiência de investimento em diferentes classes de ativos.

Faixa de Pontuação: de 170 a 229 pontos.

Perfil Agressivo: busca crescimento agressivo de capital com alta tolerância a risco e nenhuma necessidade de liquidez. Entende que os ganhos e perdas são inerentes a alocações preponderantemente em ativos de risco, aceitando perdas significativas de patrimônio na busca de retornos elevados no longo prazo. Há, em geral, muita experiência de investimento em diferentes classes de ativos.

Faixa de Pontuação: acima de 229 pontos.

Não Informado (Recusa): 'Declaro que decidi não responder ao questionário para identificação do meu Perfil de Risco e responsabilizo-me integralmente pelos efeitos desta opção estando ciente:

• da importância dos procedimentos para identificação de perfil de risco dos investidores;

• de que, ao abster-me de responder a esse questionário, a Finacap desconhecerá meu perfil de investidor, e portanto estará impossibilitada de realizar qualquer análise relativa ao enquadramento de meus investimentos, bem como não conseguirá compará-los e/ou oferecer produtos que estejam adequados ao meu perfil;

• de que me responsabilizo integralmente por quaisquer situações e problemas relativos ao meus investimentos.'

Dispensado:

• analistas, administradores de carteira e consultores de valores mobiliários autorizados pela CVM, em relação a seus recursos próprios;

• investidores não residentes (INR);

• agente autônomo de investimento, em relação a seus recursos próprios;

• investidor que tiver sua carteira de valores mobiliários administrada discricionariamente por administrador de carteira de valores mobiliários autorizado pela CVM

ASSINATURA DO COTISTA TITULAR

ANEXO II – QUESTIONARIO PESSOA JURIDICA

IDENTIFICAÇÃO DO PERFIL DO INVESTIDOR (SUITABILITY)

Razão Social do Cotista Titular CNPJ do Cotista Titular:

Data:

- Seção 1

Responda às questões abaixo escolhendo a alternativa que melhor se adequa a seu perfil, tendo em vista sua situação financeira, seus objetivos e sua tolerância a riscos. Assinale apenas uma alternativa em cada questão. Responda a todas às questões.

PARA USO DO DISTRIBUIDOR (Pontos de cada resposta)

1. Qual é a política da empresa em relação às aplicações financeiras?

a. Evita perder qualquer parcela do valor investido, mesmo que tenha rendimentos menores. [0 ponto]

b. Aceita pequenas perdas em busca de rendimentos maiores no longo prazo. [14 pontos]

c. Aceita perdas maiores em busca de rendimentos muito elevados. [20 pontos]

2. Qual é o principal objetivo das aplicações financeiras da empresa?

a. Maior parte destina-se a objetivos de curto prazo (ex: gestão do fluxo de caixa). [0 ponto]

b. Uma parte destina-se a objetivos de curto prazo e outra a objetivos de médio prazo (ex: reserva financeira, provisões). [14 pontos]

c. Maior parte destina-se a objetivos de longo prazo (ex: expansão dos negócios). [20 pontos]

3. Com quais aplicações financeiras a empresa tem familiaridade, pensando no funcionamento e nos riscos de cada uma?

a. CDB, fundos DI ou poupança. [0 ponto]

b. Além das anteriores, outros produtos de renda fixa, produtos estruturados sem perda de capital (ex: Capital Garantido) ou fundos multimercados. [2 pontos]

c. Além dos anteriores, ações, fundos de ações ou fundos imobiliários [3 pontos]

d. Além dos anteriores, também derivativos (ex: futuros, opções, produtos estruturados com risco de perda de capital) [5 pontos]

TOTAL DE PONTOS (SOMATÓRIO DOS PONTOS OBTIDOS NAS 3 QUESTÕES):

- Seção 2

Perfil Conservador: sua empresa tem objetivos de curto/médio prazo e por isso prioriza investimentos que preservam o capital e/ou o poder de compra. Investe a maior parte dos recursos em ativos de baixo risco, com alta liquidez.

Faixa de Pontuação: até 30,99 pontos.

Perfil Moderado: a sua empresa tem objetivos de médio prazo, o que permite aplicar em algum investimento de risco em busca da possibilidade de um retorno um pouco maior. Entende que os ganhos e perdas são inerentes à alocação em ativos de risco, aceitando perdas de patrimônio na busca de maiores retornos no médio e longo prazo.

Faixa de Pontuação: de 31 a 39,99 pontos.

Perfil Agressivo: sua empresa tem projetos de longo prazo, o que permite maior diversificação dos investimentos em busca de maiores retornos. Busca crescimento elevado de capital com alta tolerância a risco e baixa necessidade de liquidez. Entende que ganhos e perdas são inerentes a alocações preponderantemente em ativos de risco, aceitando perdas significativas de patrimônio na busca de retornos elevados no longo prazo.

Faixa de Pontuação: igual ou acima de 40 pontos.

Não Informado (Recusa): ‘Declaro que decidi não responder ao questionário para identificação do meu Perfil de Risco e responsabilizo-me integralmente pelos efeitos desta opção estando ciente:

• da importância dos procedimentos para identificação de perfil de risco dos investidores;

• de que, ao abster-me de responder a esse questionário, a Finacap desconhecerá meu perfil de investidor, e portanto estará impossibilitada de realizar qualquer análise relativa ao enquadramento de meus investimentos, bem como não conseguirá compará-los e/ou oferecer produtos que estejam adequados ao meu perfil;

• de que me responsabilizo integralmente por quaisquer situações e problemas relativos ao meus investimentos.’

Dispensado:

• pessoas habilitadas a atuar como integrantes do sistema de distribuição;

• companhias seguradoras e sociedades de capitalização;

• entidades abertas e fechadas de previdência complementar;

• investidores não residentes (INR);

• Pessoas Jurídicas que sejam consideradas investidores qualificados, conforme regulamentação específica;

• instituição financeira ou instituição autorizada a funcionar pelo Banco Central do Brasil;

- Pessoa Jurídica de Direito Público;

- investidor que tiver sua carteira de valores mobiliários administrada discricionariamente por administrador de carteira de valores mobiliários autorizado pela CVM;

- analistas, administradores de carteira, consultores de valores mobiliários autorizados pela CVM e agente autônomo de investimento, em relação a seus recursos próprios.

ASSINATURA DO COTISTA TITULAR

ANEXO III – TERMO DE CIÊNCIA DE QUESTIONÁRIO (TCQ)

INFORMAÇÕES DO CLIENTE:

Nome:

CPF/CNPJ:

Prezado Cliente,

Antes de realizar o investimento descrito abaixo é importante que você verifique se ele está de acordo com os seus objetivos. Para isso precisamos conhecer o seu perfil de investidor.

Fundo:

CNPJ:

Perfil de Risco do Fundo (ex: agressivo):

Ao datar e assinar esta declaração, você terá confirmado (i) ter plena ciência da importância de conhecer seu perfil de investidor para apoiar sua decisão de investimento e que enquanto não conhecer o seu perfil não poderá receber recomendação de investimento; (ii) que não deseja conhecer seu perfil de investidor neste momento e tem ciência de que isso implica em não receber recomendação de investimento, enquanto não conhecer o seu perfil; e (iii) ter plena ciência de que as operações eventualmente contratadas podem possuir riscos maiores do que aqueles previstos nos produtos que seriam recomendados para o seu perfil;

Ciente e de acordo em / / :

_____

Assinatura do Cliente

ANEXO IV – TERMO DE CIÊNCIA DE DESENQUADRAMENTO (TCD)

INFORMAÇÕES DO CLIENTE:

Nome:

CPF/CNPJ:

Perfil do investidor:

Prezado Cliente,

O investimento descrito abaixo é inadequado ao seu perfil de investidor. Ao prosseguir com o investimento neste fundo você assumirá riscos maiores do que aqueles previstos nos produtos adequados ao seu perfil.

Fundo:

CNPJ:

Perfil de Risco do Fundo (ex: agressivo):

Ao datar e assinar esta declaração, você terá confirmado sua plena ciência de que a operação contratada não é compatível com seu perfil de investidor, bem como que leu e entendeu o teor de todas as informações sobre o fundo, especialmente sobre os riscos do investimento.

Ciente e de acordo em / / :

_____

Assinatura do Cliente

ANEXO V - GOVERNANÇA DE PRODUTOS POR PERFIL DE INVESTIDOR – LISTA NEGATIVA

Produtos/Perfil do Cliente	I Conservador	II Moderado	III Arrojado	IV Agressivo
Fundo de Ações	RESTRITO	-	-	-
FII	-	-	-	-
Incorporação	VEDADO	-	-	-
Imóveis prontos	RESTRITO	-	-	-
Títulos Privados	RESTRITO	-	-	-
FIP	-	-	-	-
Fundos Private Equity	VEDADO	VEDADO	-	-
FIDC	RESTRITO	-	-	-
Fundos Estruturados c/ risco de perda de capital	VEDADO	-	-	-
Fundos indexados à inflação	RESTRITO	-	-	-
Fundos Offshore	RESTRITO	-	-	-
Fundos c/ cota valorizada diferente de diária e pgto resgate superior a 180 dias	RESTRITO	RESTRITO	RESTRITO	-

Legenda:

RESTRITO – Proibida a recomendação, mas permitida a aquisição por solicitação do cliente.

VEDADO – Proibidas a recomendação e a aquisição por solicitação do cliente.

ANEXO VI – PRODUTOS COMPLEXOS

- Cotas de FIP / FIDC / FII

- Cotas de Fundos Estruturados

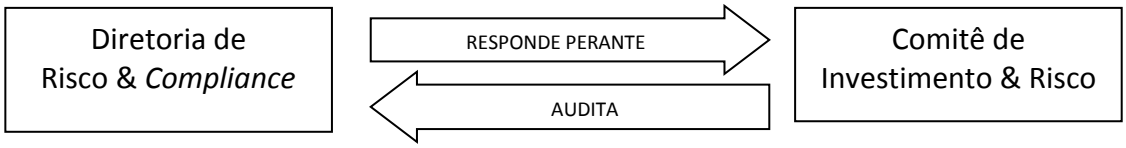
- Cotas de Fundos Multimercado e cotas de Fundos Offshore, ambos com frequência de cálculo de cota diferente de diária e prazo para pagamento de resgate superior a 180 dias corridos.

MANUAL DE GESTÃO E CONTROLE DE RISCO

1. Introdução

A Finacap tem como filosofia a gestão e controle dos riscos inerentes ao seu negócio e se compromete em manter as melhores práticas para o sucesso do negócio e a seleção das melhores oportunidades de investimento. Levando isso em conta, a Finacap adota práticas e políticas que possibilitam realizar suas atividades com níveis de risco alinhados a capacidade operacional da empresa e a tolerância a risco de seus clientes/investidores.

O processo de gestão e controle de risco conta com duas unidades, uma de administração (Diretoria de Risco e *Compliance)* e outra de auditoria (Comitê de Investimento & Risco), garantindo uma visão e entendimento adequado dos riscos do negócio, para que as operações e o desempenho não sejam afetados. Além disso, o processo de gestão de risco visa proporcionar aos clientes da Finacap um maior conforto em relação aos seus investimentos.



2. Fundamentos da Análise de Risco

A Finacap tem em mente três fundamentos básicos para a gestão e controle de risco e leva em consideração:

I. Retorno;
II. Risco;
III. Incerteza.

O Retorno tem por definição a apuração do ganho de capital ao final do período de investimento.

O Risco contém todas as incertezas associadas ao retorno de um investimento e contém eventos, previstos ou não, que podem ter um impacto no retorno esperado.

A Incerteza refere-se ao grau de assertividade de determinada decisão, após a avaliação risco x retorno de um investimento. Ou seja, o risco pode ser definido como uma tentativa de se medir o grau de incerteza para a obtenção do retorno.

3. Risco de Mercado

Risco de mercado é definido como a possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de posições detidas pela Finacap. O risco de mercado inclui operações sujeitas á variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities). O risco de mercado, também conhecido como risco sistemático, também pode ser definido pelo risco de uma reação em cadeia atingir e danificar todo o sistema financeiro de um país ou região. Podendo ser causado, por exemplo, pela falência de uma grande instituição financeira, gerando um efeito dominó.

Para uma sólida gestão de risco de mercado, os gestores monitoram e controlam os riscos de variações nas cotações de mercado dos instrumentos financeiro com a finalidade de otimizar a relação retorno-risco. Tudo isso, porém, levando em conta os limites, modelos e políticas relacionadas à gestão de recursos na Finacap.

4. Risco de Liquidez

Risco de liquidez pode ser dividido entre duas formas distintas:

- Risco de liquidez de ativos ou mercado: é o risco de um instrumento financeiro de investimento não poder ser negociado com rapidez suficiente ou pelo preço justo de mercado. Este tipo de risco de liquidez acontece geralmente com ativos que não são amplamente negociados no mercado de capitais, o que acarreta em dificuldades de encontrar compradores ou vendedores para o ativo que o ativo seja negociado em um determinado momento.
- Risco de liquidez de *funding* ou fluxo de caixa: associado à possibilidade de não possuir recursos financeiros (caixa) em um momento previsto para honrar com seus compromissos e com isso tornando suas obrigações financeiras inadimplentes.

Para a análise de liquidez, a Finacap leva em consideração não só o valor esperado de venda dos ativos de uma determinada carteira, mas também a quantidade em tempo em que esses ativos podem ser convertidos em caixa. A Finacap elabora projeções de fluxo de caixas, levando em conta todos os ativos, passivos e recebíveis de suas carteiras para ajustar seus níveis de exposição ao risco de liquidez.

A modelagem de fluxo de caixa visa a verificar o fluxo de caixa temporal de todos os ativos (principal e juros) e passivos, de acordo com as características das transações da Finacap. Esta análise será utilizada na avaliação da liquidez da Finacap, uma vez que permite mapear todos os ativos e passivos desta no horizonte de tempo. Partindo-se da data de

análise, a Finacap deve ter ativos suficientes para cobrir os passivos, ou seja, o valor esperado de cada um dos fluxos deve ser maior que zero.

A metodologia utilizada pela Finacap para mitigar esse tipo de risco visa apurar o valor necessário para cobrir eventuais resgates líquidos fora do padrão histórico, apresentado em forma de percentual do patrimônio líquido, com base nas características de liquidez dos ativos e nos resgates não convencionais nos últimos 3 anos, estabelecendo assim, limites para esse risco.

5. Risco de Crédito

Define-se como risco de crédito a possibilidade de ocorrências de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remuneração, às vantagens concedidas na renegociação e aos custos de recuperação.

O Comitê de Investimento e Risco monitora de forma centralizada os riscos inerentes aos investimentos das carteiras da Finacap, utilizado indicadores de risco e desempenho. Isso garante o alinhamento entre as estratégias definidas pela organização e eventuais mudanças no cenário macroeconômico e de credito.

Os processos de gestão e controle de risco de crédito são reavaliados periodicamente, a fim de mantê-los alinhados às melhores práticas de mercado e aderentes aos processos de melhoria contínua. Além da análise do risco de crédito em si, ainda são analisadas questões como concentração por cliente, grupo econômico, produto e retornos ajustados pelo risco.

Associado ao risco de crédito está o risco de contraparte, também conhecido como risco de *default que,* pode ser definido como o risco de perda pela incapacidade de pagamento do tomador de um empréstimo, contraparte de um contrato ou emissor de um título. Desta forma, é essencial que o emissor de um título seja exaustivamente analisado, para que o risco de contraparte seja menor.

É um risco bilateral sobre uma contraparte com a qual uma ou mais operações de mercado tenham sido realizadas. O valor de exposição a este risco pode variar ao longo do tempo em função dos parâmetros de mercado que impactam o instrumento negociado.

6. Risco de Concentração

O risco de concentração de crédito pode ser definido como o risco de perdas em decorrência da não diversificação de risco de crédito de investimentos. Exemplos de risco de concentração são dados pela alocação dos recursos disponíveis em um número pequeno de emissores do mesmo setor econômico, classes de ativos e posse de parte substancial dos passivos de um emissor. A mitigação deste tipo de risco é feita pela pulverização do risco entre variados emissores e classes de ativos.

O gerenciamento desse tipo de risco permite identificar sob diferentes óticas e para diferentes variáveis o excesso ou o reduzido posicionamento, em, por exemplo: patrimônio líquido, captações, resgates, ativos financeiros, emissores e, ainda, características particulares dos clientes ou cotistas de cada veículo de investimento em relação a si mesmo ou de forma integral.

Os objetivos do gerenciamento do risco de concentração para carteiras, clubes e fundos geridos são: aderência aos normativos de órgãos de controle e de boas práticas, identificação de pontos de excesso ou de mínimos que possam implicar perdas e motivação para áreas de gestão de ativos, de risco e comercial no sentido de corrigir eventuais desajustes ou convergência para obtenção de resultados.

7. Risco Operacional

O risco operacional tem como características a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, danos à infraestrutura de suporte, utilização indevida de modelos ou produtos, alterações no ambiente de negócios, situações adversas de mercado ou qualquer tipo de evento não previsto que torne impróprio o exercício das atividades da Finacap.

O processo de gerenciamento de riscos operacionais segue as seguintes etapas: mapeamento de processos e identificação dos recursos necessários para realização das atividades do negócio, identificação e tratamento dos riscos com avaliações quantitativas com base em número de erros, probabilidade de ocorrência e impacto causado, implementação de estratégias de melhoria dos processos visando mitigar ou eliminar os riscos, e, por fim, o monitoramento dos controles, que visa verificar se as estratégias de controle estão sendo cumpridas e a mitigação do risco operacional está implementada de acordo com o plano de gerenciamento proposto.

ANEXO VIII – TERMO DE CIÊNCIA E COMPROMISSO

TERMO DE CIÊNCIA E COMPROMISSO
MANUAL DE CONTROLES INTERNOS

Declaro ter lido, cópia do MANUAL DE CONTROLES INTERNOS, comprometendo-me observá-lo, aceitar, atender e cumpri-lo em sua íntegra e comunicar imediatamente a qualquer ato ou ação de descumprimento das regras e procedimentos contidos no mesmo.

Declaro também, estar ciente de que o descumprimento de qualquer norma ou procedimento contido no MANUAL DE CONTROLES INTERNOS, implicará na adoção de medidas disciplinares pela FINACAP.

Recife, de 20____

Nome:

CPF:

Assinatura: